

VERSION	ITEM	DESCRIPTION
V-1	VERSION	VERSION OF FORMAT OF CERTIFICATE
	SERIAL NUMBER	CERTIFICATE NUMBER ASSIGNED BY CERTIFICATE ISSUER
	SIGNATURE	SIGNATURE ALGORITHM OF CERTIFICATE
	ISSUER	NAME OF CERTIFICATE ISSUER (DISTINGUISHED NAME FORMAT)
	VALIDITY START END	PERIOD IN WHICH CERTIFICATE IS VALID STARTING DATE AND TIME ENDING DATE AND TIME
	SUBJECT	NAME OF HOLDER OF CERTIFICATE
	SUBJECT PUBLIC KEY INFORMATION ALGORITHM SUBJECT PUBLIC KEY	PUBLIC KEY INFORMATION OF HOLDER OF CERTIFICATE ALGORITHM OF KEY KEY

FIG. 2

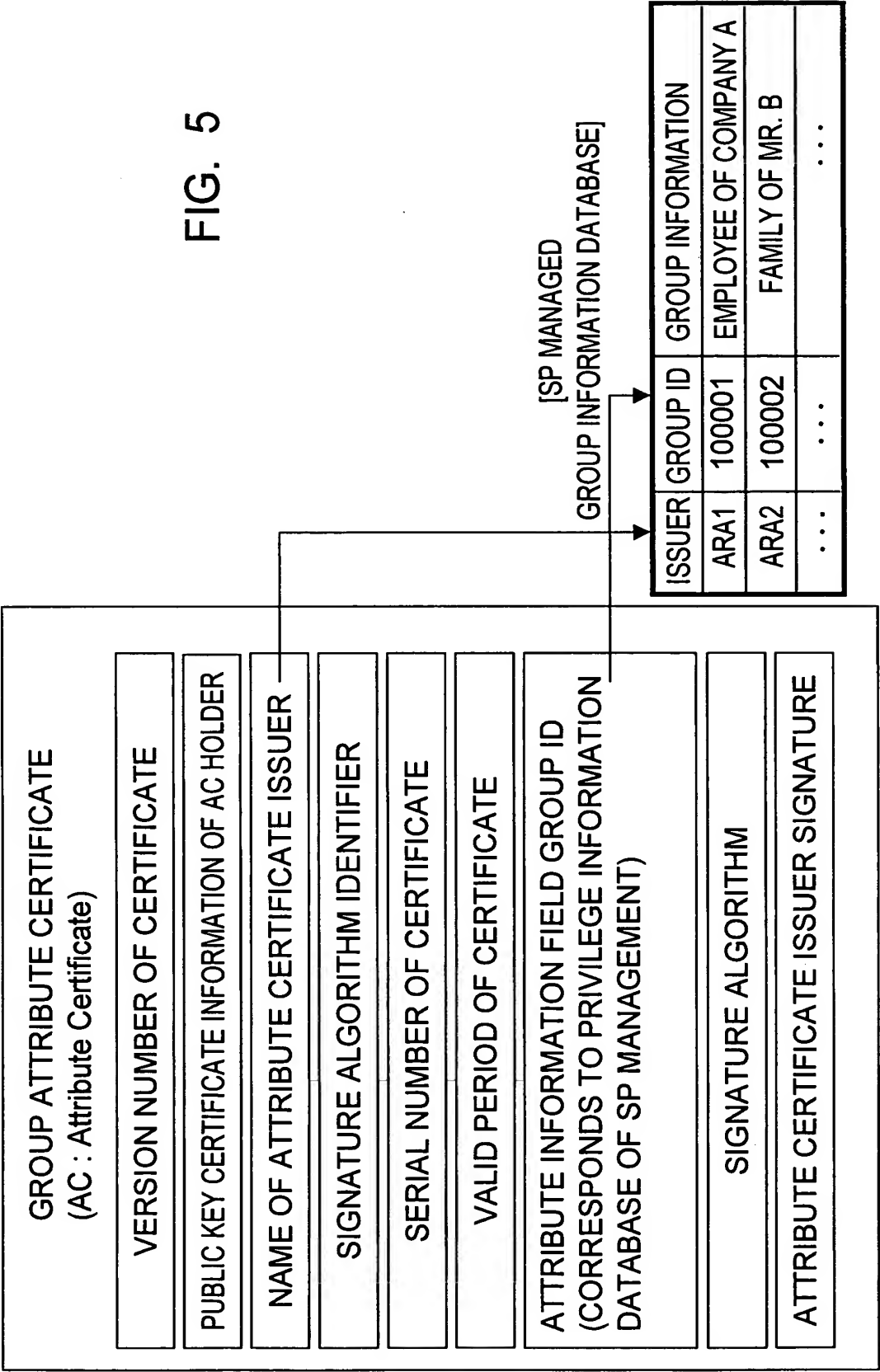
FIG. 3

V-3	AUTHORITY KEY IDENTIFIER KEY IDENTIFIER AUTHORITY CERTIFICATE ISSUER NAME AUTHORITY CERTIFICATE SERIAL NUMBER	KEY IDENTIFIER OF CERTIFICATE ISSUER USED FOR SIGNATURE VERIFICATION KEY IDENTIFIER ORGANIZATION CERTIFICATE ISSUER NAME (GENERAL NAME FORMAT) ORGANIZATION CERTIFICATE SERIAL NUMBER
	SUBJECT KEY IDENTIFIER KEY IDENTIFIER	CLEARLY IDENTIFY OBJECT KEY FROM MULTIPLE KEYS
	KEY USAGE (0) DIGITAL SIGNATURE (1) NON-REPUDIATION (2) KEY ENCIPHERMENT (3) DATA ENCIPHERMENT (4) KEY AGREEMENT (5) KEY CERT SIGNATURE (6) cRL SIGNATURE	SPECIFY USAGE OF KEY (0) FOR DIGITAL SIGNATURE (1) FOR PREVENTING REPUDIATION (2) FOR ENCIPHERING KEY (3) FOR ENCIPHERING MESSAGE (4) FOR DISTRIBUTING SHARED KEY (5) FOR CONFIRMING SIGNATURE OF CERTIFICATION (6) FOR CONFIRMING SIGNATURE OF REVOCATION LIST
	SECRET KEY VALIDITY START END	VALID PERIOD FOR SECRET KEY CORRESPONDING TO PUBLIC KEY IN CERTIFICATE
	CERTIFICATE POLICY POLICY IDENTIFIER POLICY QUALIFIER	CERTIFICATE POLICY ACKNOWLEDGED BY CERTIFICATE ISSUER POLICY ID (ISO/IEC9834-1 COMPLIANT) AUTHENTICATION STANDARD
	POLICY MAPPING ISSUER DOMAIN POLICY SUBJECT DOMAIN POLICY	RESTRICTION OF RELATION OF POLICIES IN AUTHENTICATION PATH

FIG. 4

V-3	SUBJECT ALTERNATE NAME	ALTERNATIVE NAME FOR CERTIFICATE HOLDER (GN FORMAT)
	ISSUER ALTERNATIVE NAME	ALTERNATIVE NAME FOR CERTIFICATE ISSUER(GN FORMAT)
	SUBJECT DIRECTORY ATTRIBUTE	ATTRIBUTE OF DIRECTORY NECESSARY FOR CERTIFICATE HOLDER
	BASIC CONSTRAINT CA PATH LENGTH CONSTRAINT	DISTINGUISH WHETHER PUBLIC KEY FOR CERTIFICATION IS FOR SIGNATURE OF CERTIFYING AUTHORITY, OR BELONGS TO CERTIFICATE HOLDER
	NAMING CONSTRAINT PERMITTED SUBTREES BASE MINIMUM MAXIMUM EXCLUSION CONSTRAINT	RESTRICTS NAME OF CERTIFICATE ISSUED BY ISSUER
	POLICY CONSTRAINT REQUIRE EXPLICIT POLICY INHIBIT POLICY MAPPING	RESTRICTS RELATIONS OF POLICIES IN AUTHENTICATION PATH
	CRL DISTRIBUTION POINT	DESCRIBES DISTRIBUTION POINTS OF REVOCATION LIST FOR CONFIRMING WHETHER OR NOT CERTIFICATE HAS BEEN REVOKED AT TIME OF CERTIFICATE HOLDER USING CERTIFICATE
	SIGNATURE ALGORITHM	ALGORITHM USED FOR ATTACHING SIGNATURE TO CERTIFICATE
	SIGNATURE VALUE	SIGNATURE BY SECRET KEY OF CERTIFICATE ISSUER

FIG. 5



ISSUER	HOLDER	VERIFIER	ATTRIBUTE INFORMATION
GROUP ARA	SC, USC	SP_SM	GROUP ID

FIG. 6

GROUP ID	GROUP INFORMATION	ISSUING POLICY
1234-0	GAME DISTRIBUTION SERVICE MEMBER	<ul style="list-style-type: none">• OWNS AUTHORIZED GAME MACHINE CONFIRMED WITH EE PKC, ETC• ALREADY PAID GAME DISTRIBUTION SERVICE JOINING FEE
1234-5-10	10-GAME USAGE MEMBER	<ul style="list-style-type: none">• MEMBER OF GAME DISTRIBUTION SERVICEOWNS GAME DISTRIBUTION SERVICE MEMBER AC• AGREED TO LIMIT TO 10 TIMES
...

FIG. 7

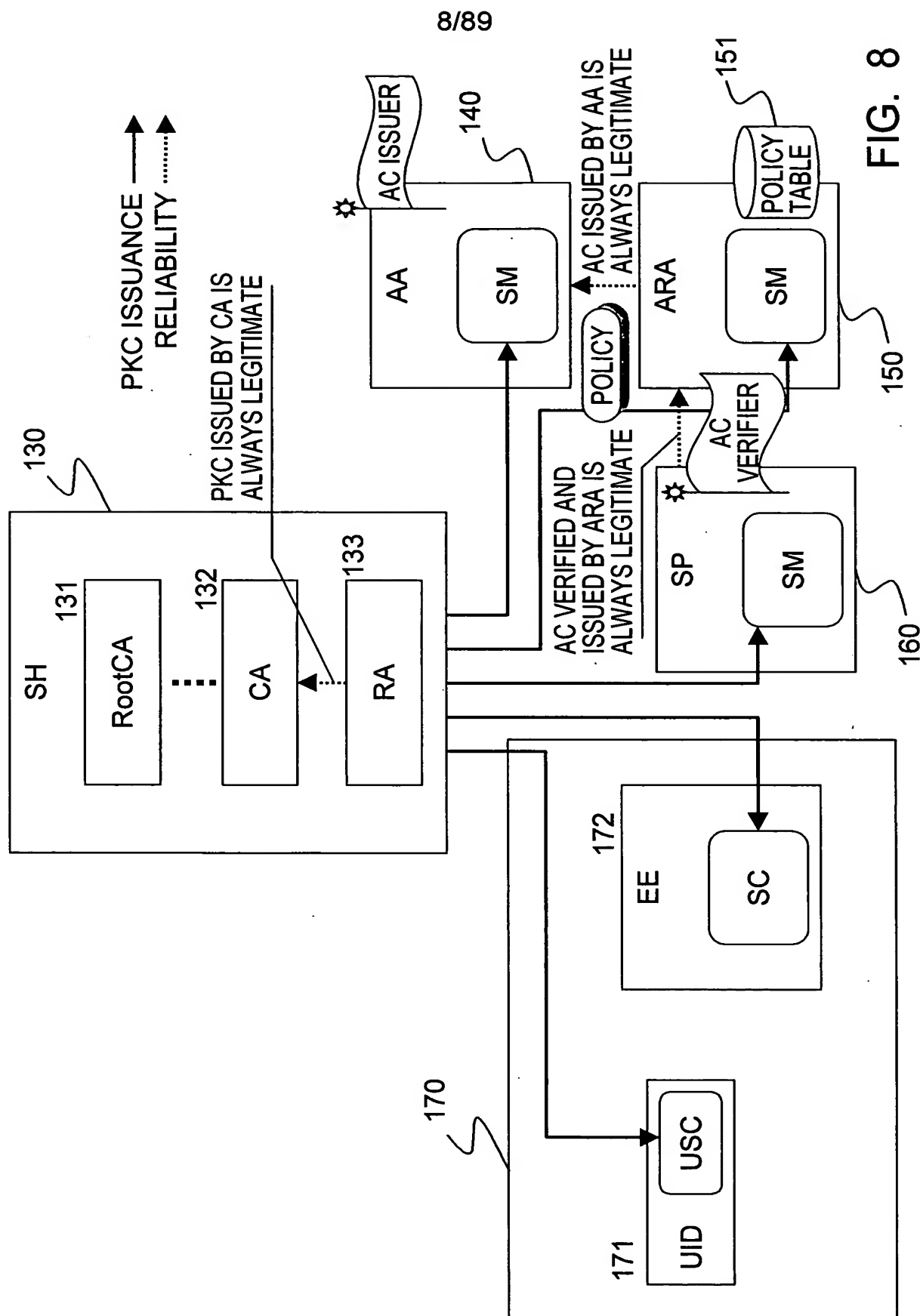


FIG. 8

9/89

SP ↔ COMMUNICATION NETWORK EXTERNAL DEVICE (EE, UID)

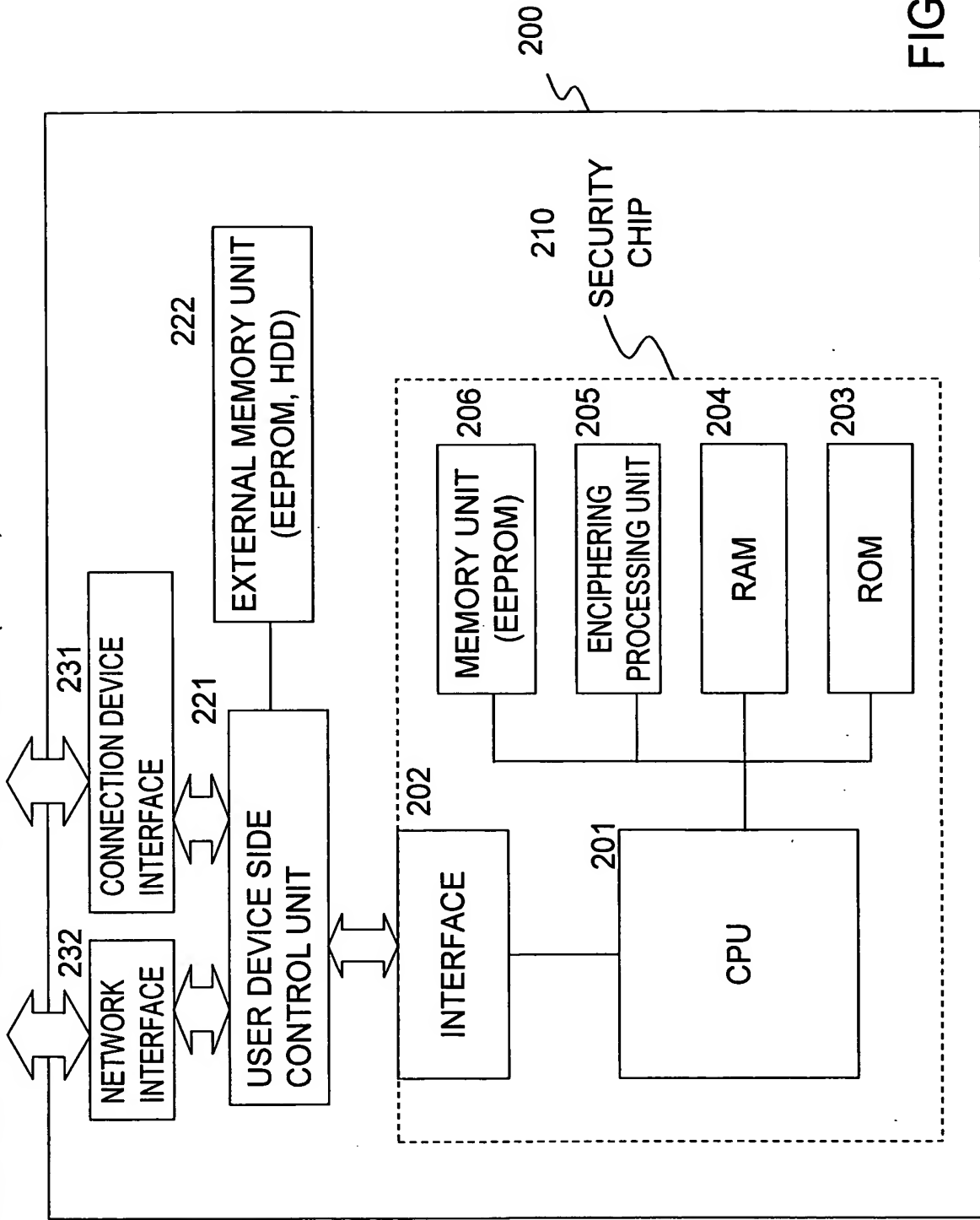


FIG. 9

DATA TYPE	DATA CONTENTS
PUBLIC KEY CERTIFICATE	<ul style="list-style-type: none">• ROUTE CERTIFICATION AUTHORITY PUBLIC KEY CERTIFICATE• SERVICE PROVIDER PUBLIC KEY CERTIFICATE
GROUP ATTRIBUTE CERTIFICATE	<ul style="list-style-type: none">• ATTRIBUTE CERTIFICATE CORRESPONDING TO GROUP TO WHICH DEVICE BELONGS OR USER BELONGS
EXECUTION ATTRIBUTE CERTIFICATE	<ul style="list-style-type: none">• ATTRIBUTE CERTIFICATE CONTAINING ADDRESS DATA OF MEMORY STORING ENCRYPTING COMMAND AND DECRYPTING REGISTRATION KEY OF ENCRYPTING COMMAND
KEY DATA	<ul style="list-style-type: none">• SECURITY CHIP PUBLIC KEY, SECRET KEY PAIR• REGISTRATION KEY• RESET KEY• RANDOM NUMBER GENERATING KEY, • MUTUAL AUTHENTICATION KEY
IDENTIFICATION INFORMATION	<ul style="list-style-type: none">• SECURITY CHIP ID• SERVICE PROVIDER ID• USER ID• APPLICATION ID
OTHERS	<ul style="list-style-type: none">• RANDOM NUMBER SEED• SERVICE USAGE INFORMATION, ETC.

FIG. 10

11/89

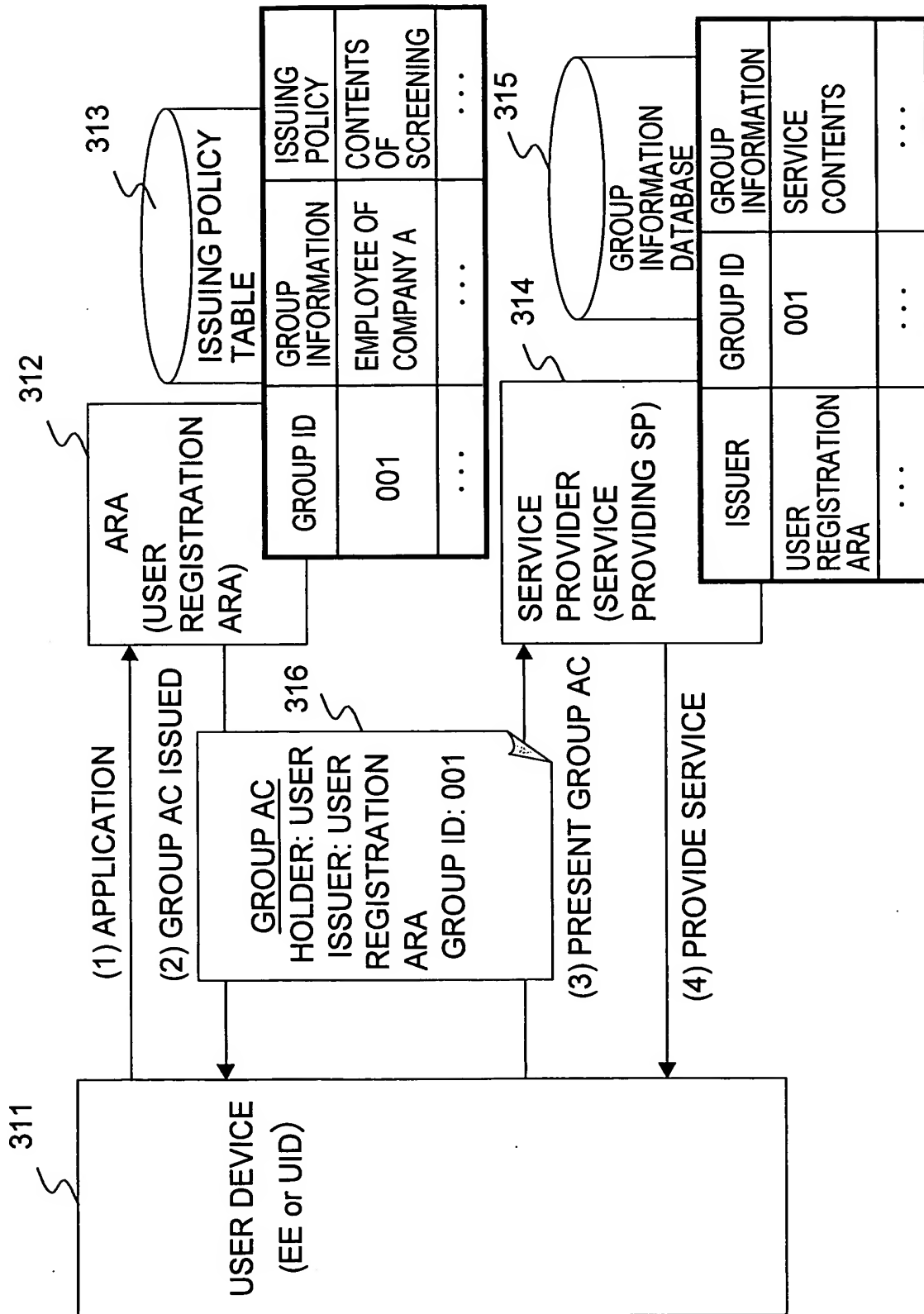
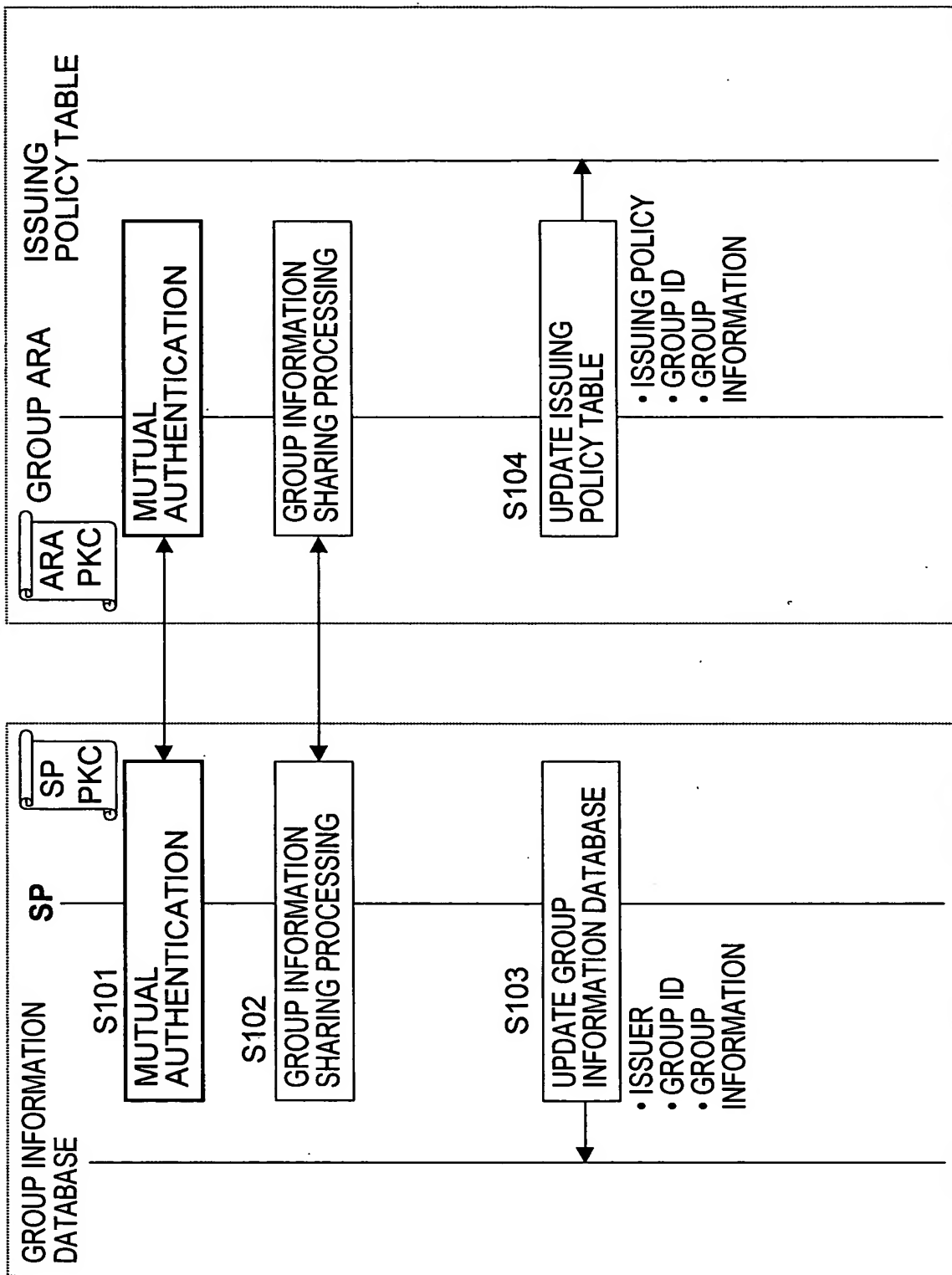


FIG. 11

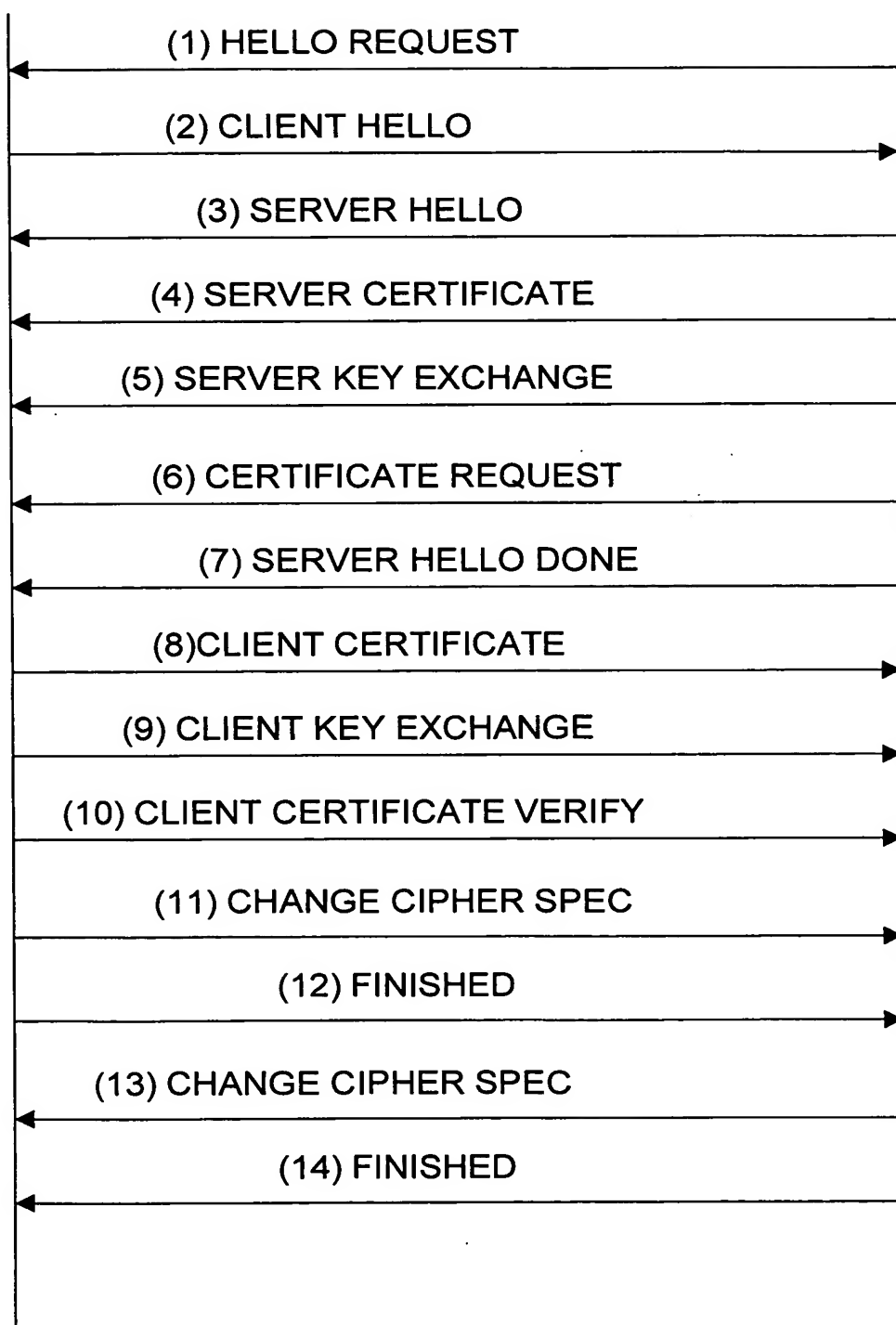
12/89

FIG. 12



13/89

FIG. 13

ENTITY A
(CLIENT)ENTITY B
(SERVER)

14/89

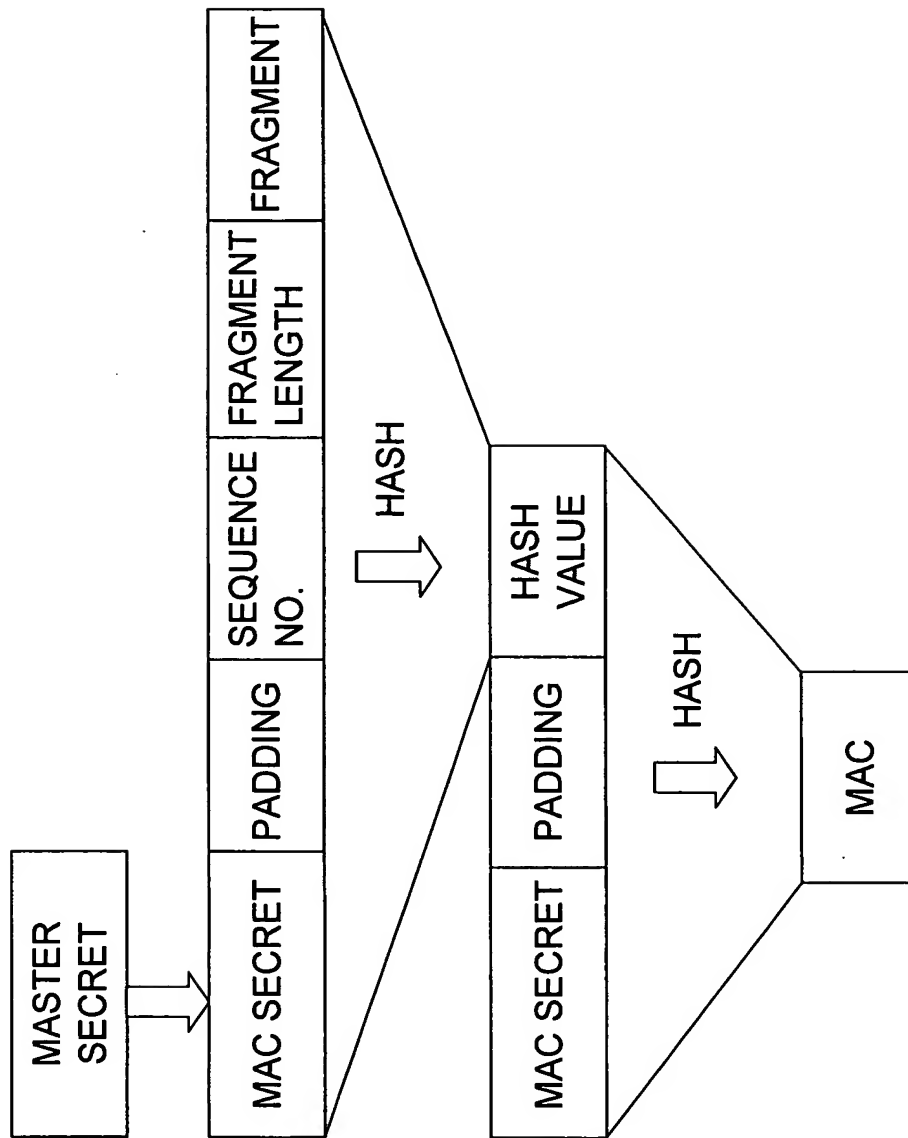


FIG. 14

(A) ISSUING POLICY TABLE (HELD BY ARA)

GROUP ID	GROUP INFORMATION	ISSUING POLICY
1234-0	GAME DISTRIBUTION SERVICE MEMBER	<ul style="list-style-type: none">• OWNS AUTHORIZED GAME MACHINE• CONFIRMED WITH EE PKC, ETC• ALREADY PAID GAME DISTRIBUTION SERVICE JOINING FEE
1234-5-10	10-GAME USAGE MEMBER	<ul style="list-style-type: none">• MEMBER OF GAME DISTRIBUTION SERVICE• OWNS GAME DISTRIBUTION SERVICE MEMBER AC• AGREED TO LIMIT TO 10 TIMES

341

342

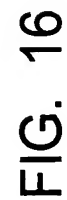
(B) GROUP INFORMATION DATABASE (HELD BY SP)

ISSUER	GROUP ID	GROUP INFORMATION
MANUFACTURER	1001	MAINTENANCE: FULL-SERVICE SUBSCRIBER
MANUFACTURER	1002	MAINTENANCE: TRIAL
GAME DISTRIBUTION SERVICE	1234-0	GAME DISTRIBUTION SERVICE MEMBER
GAME DISTRIBUTION SERVICE	1234-5-10	10-GAME USAGE MEMBER
TANAKA FAMILY, HEAD	001	TANAKA FAMILY, FAMILY
TANAKA FAMILY, HEAD	002	TANAKA FAMILY, CHILDREN

351

352

FIG. 15



17/89

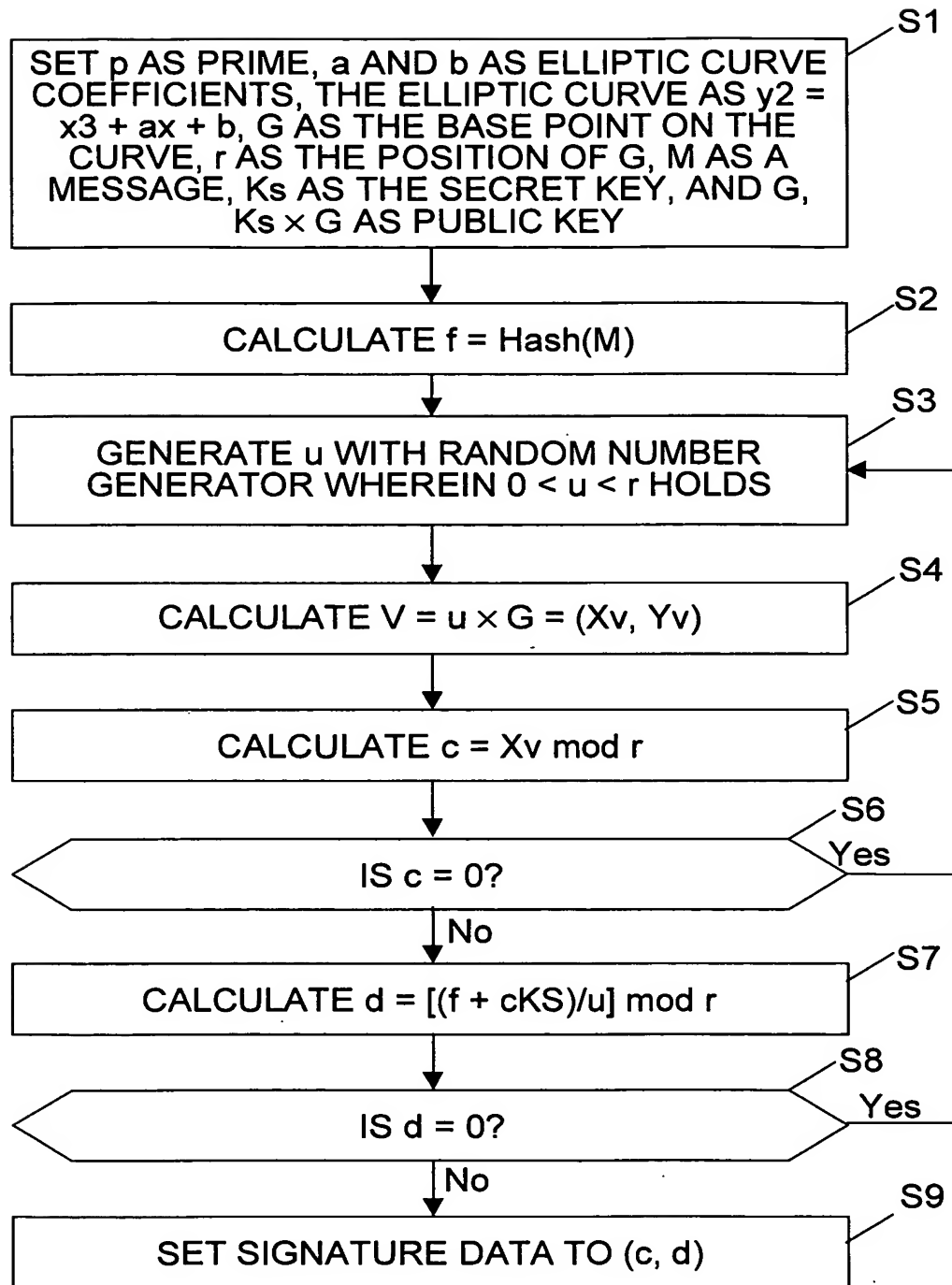


FIG. 17

18/89

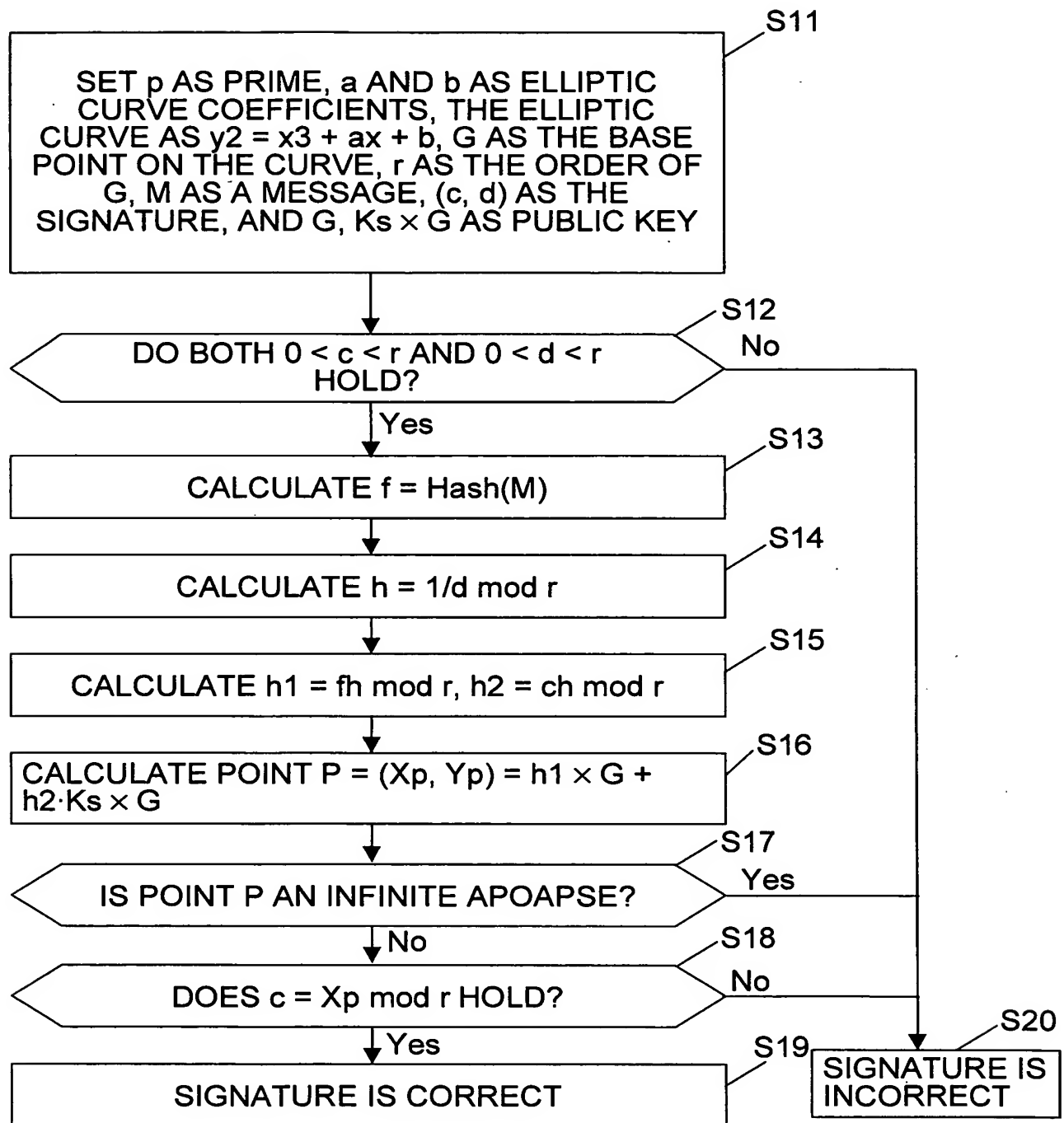


FIG. 18

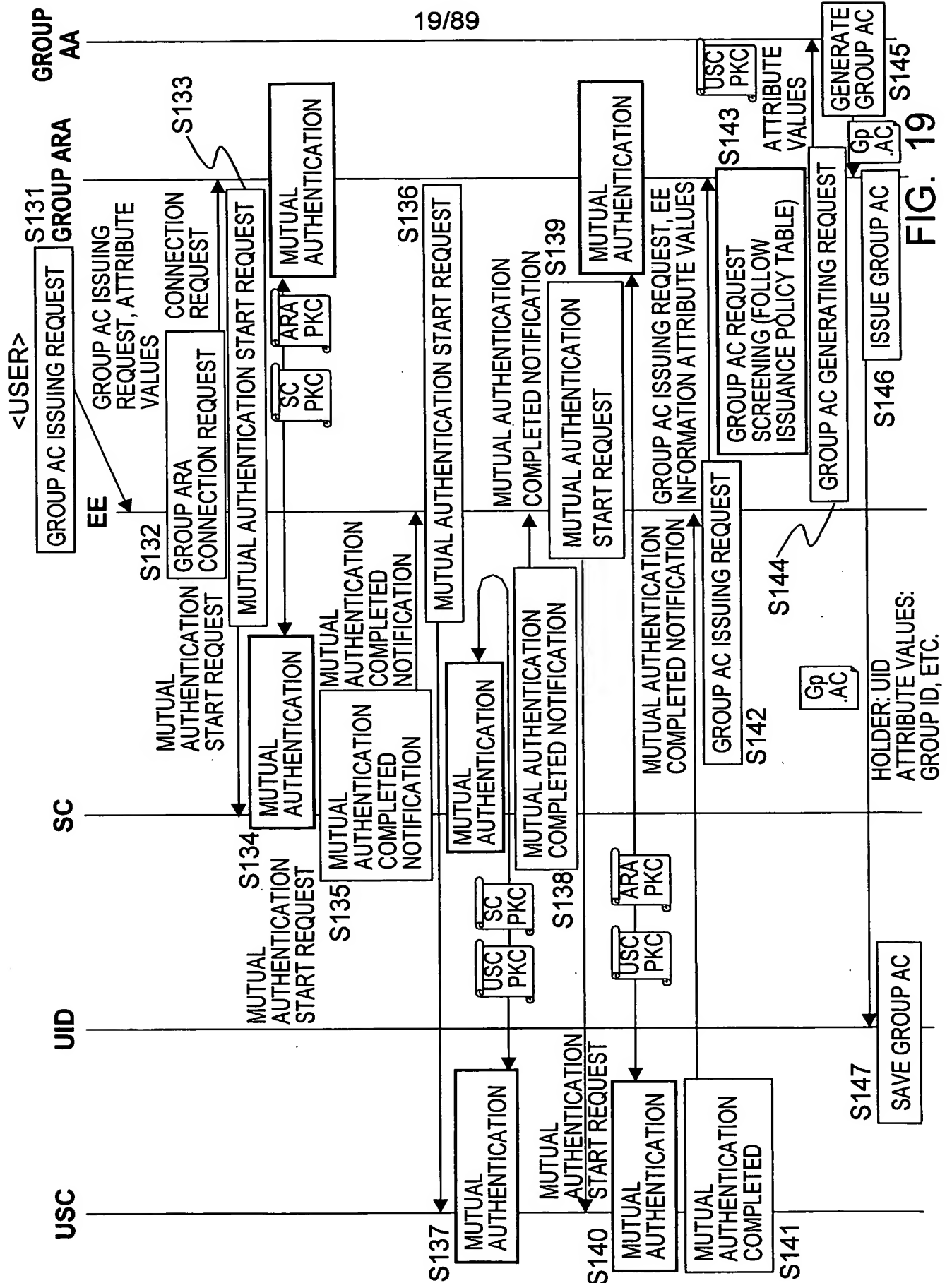


FIG. 19

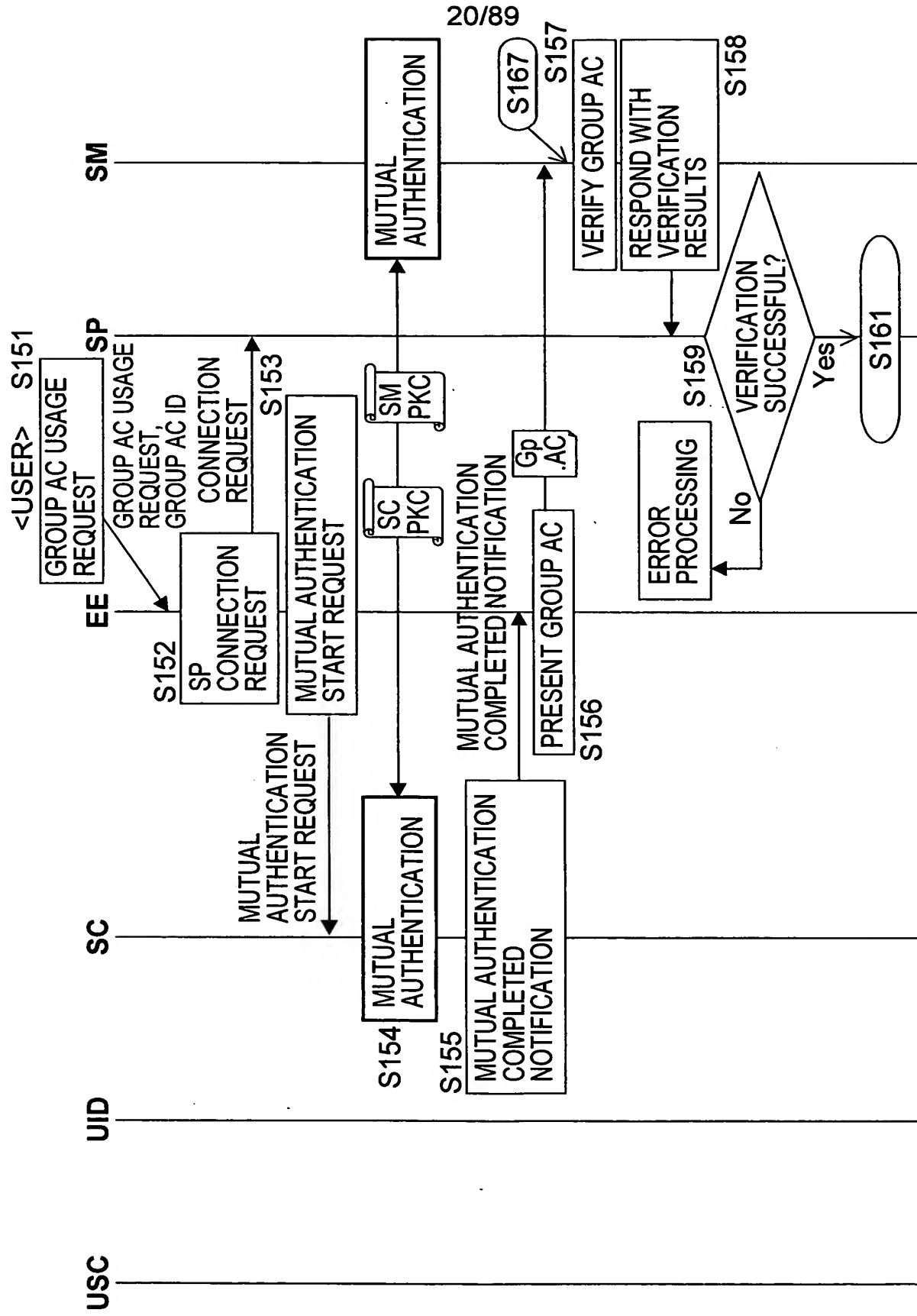


FIG. 20

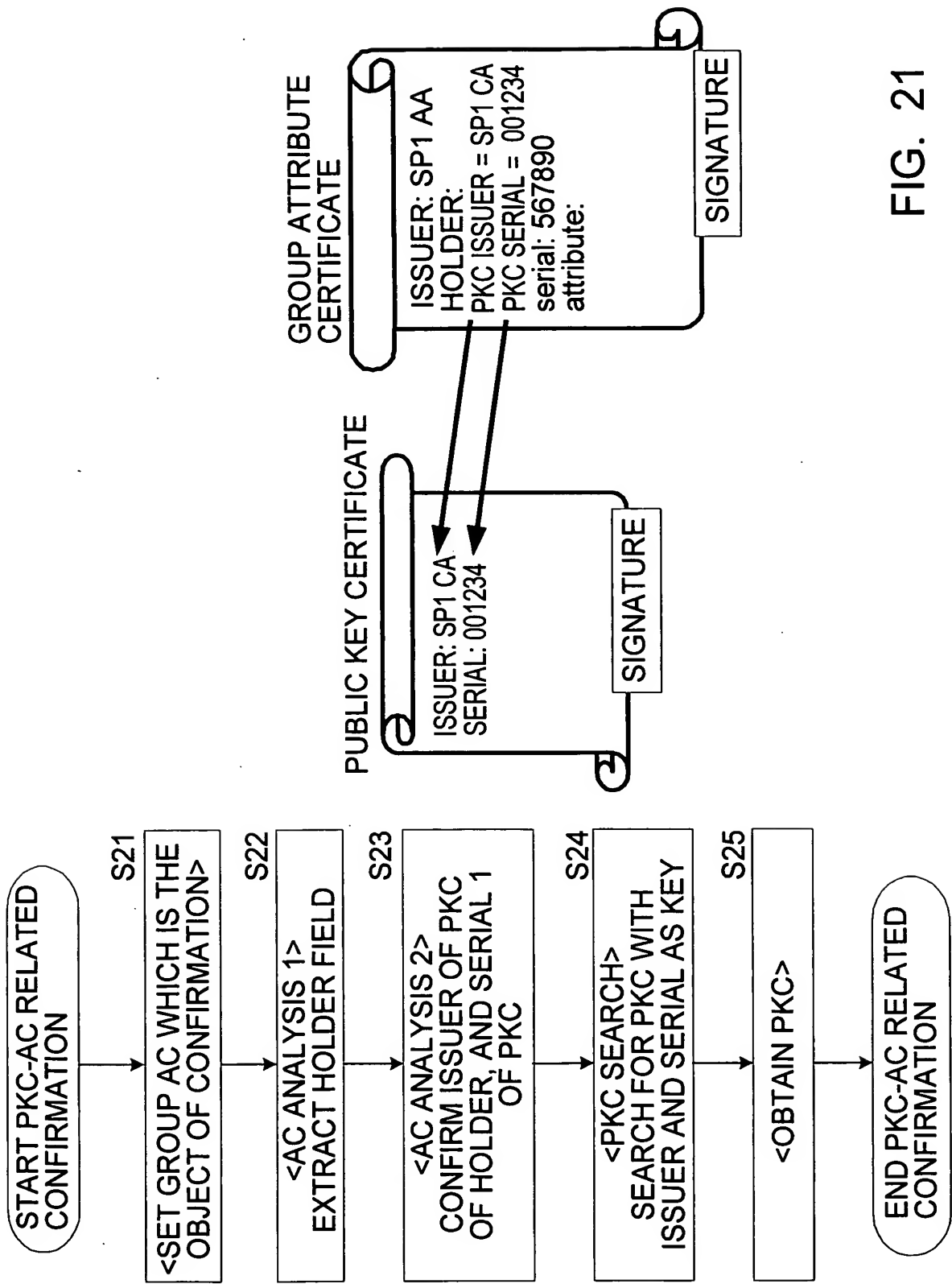


FIG. 21

22/89

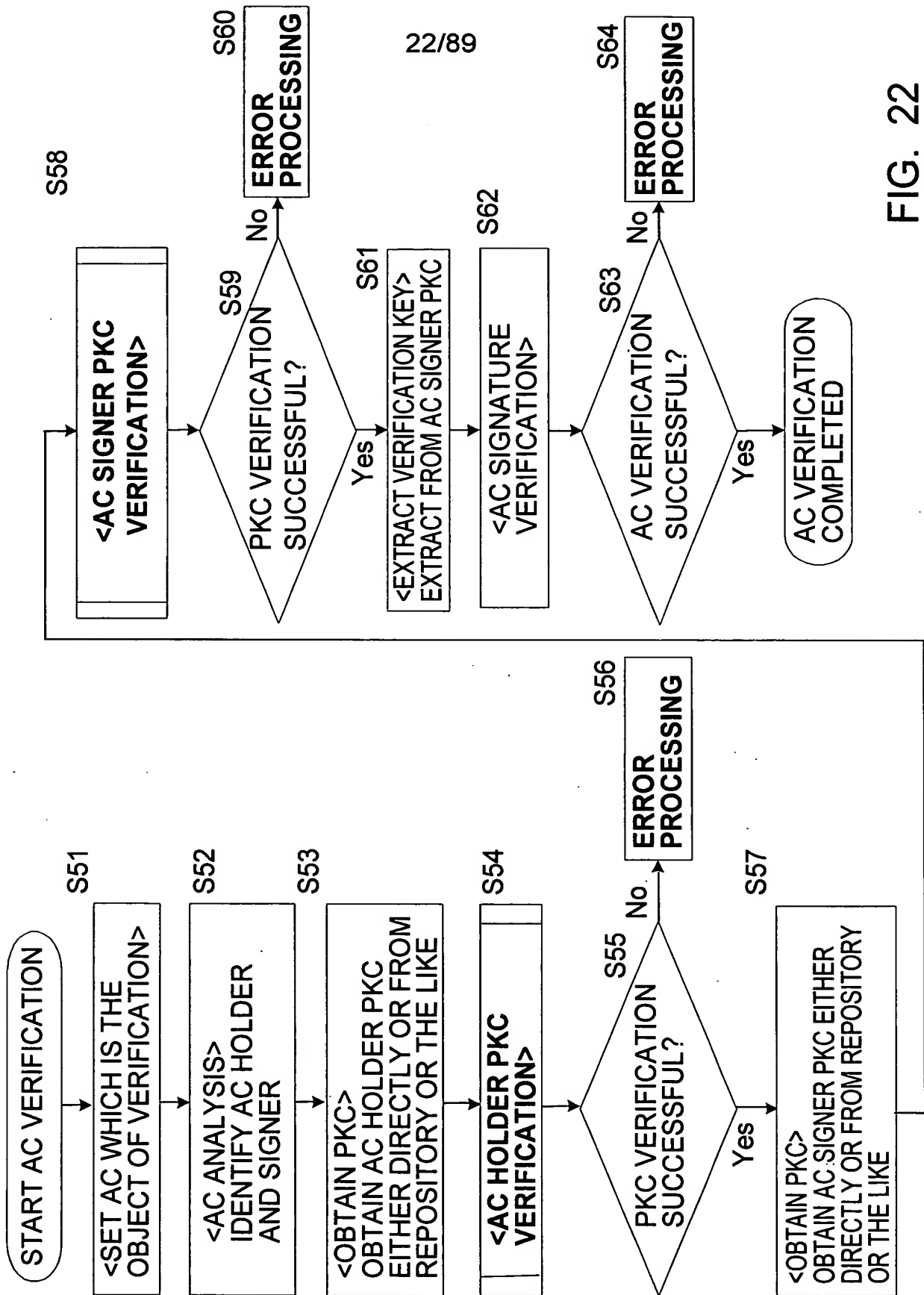


FIG. 22

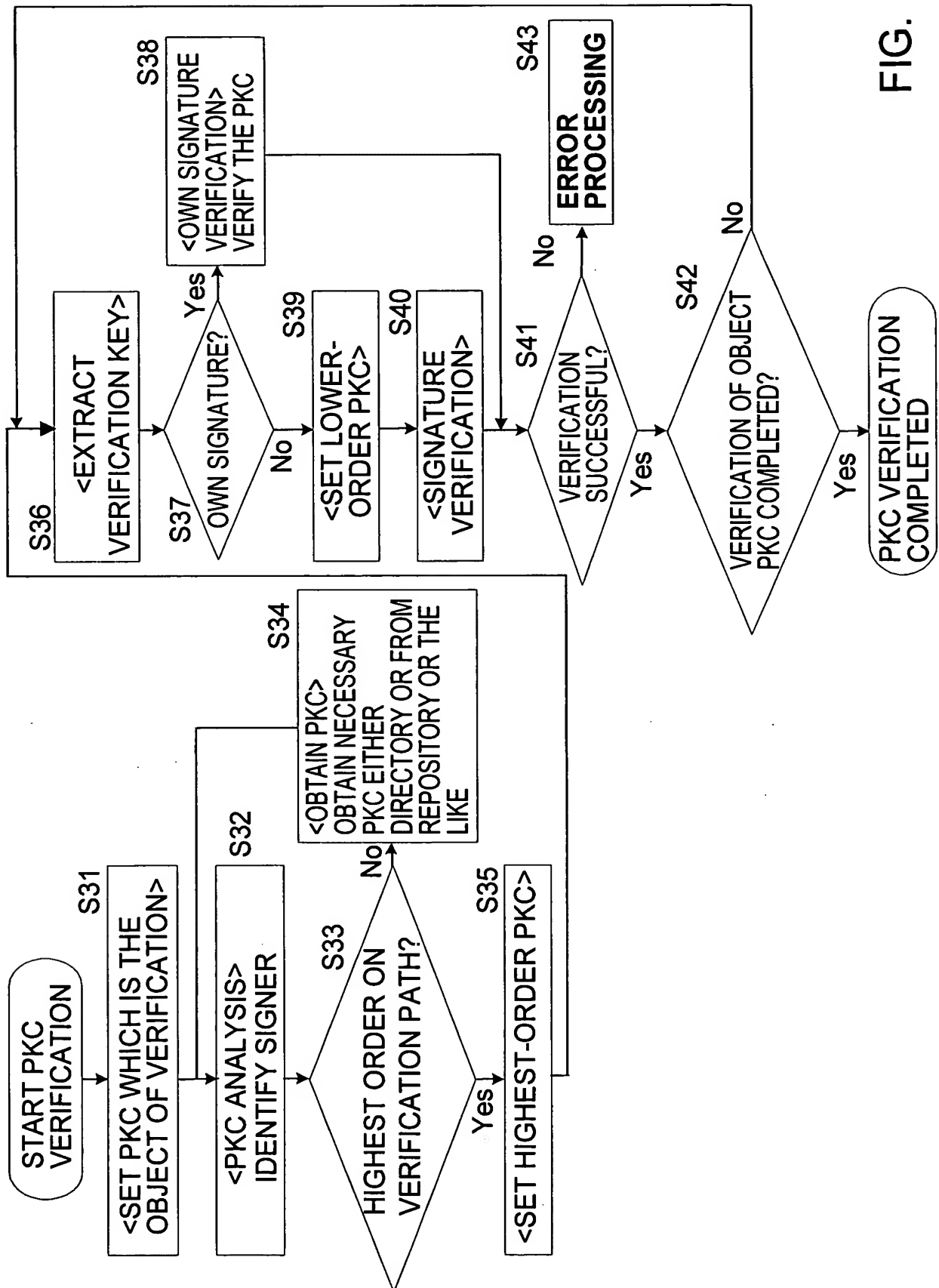


FIG. 23

24/89

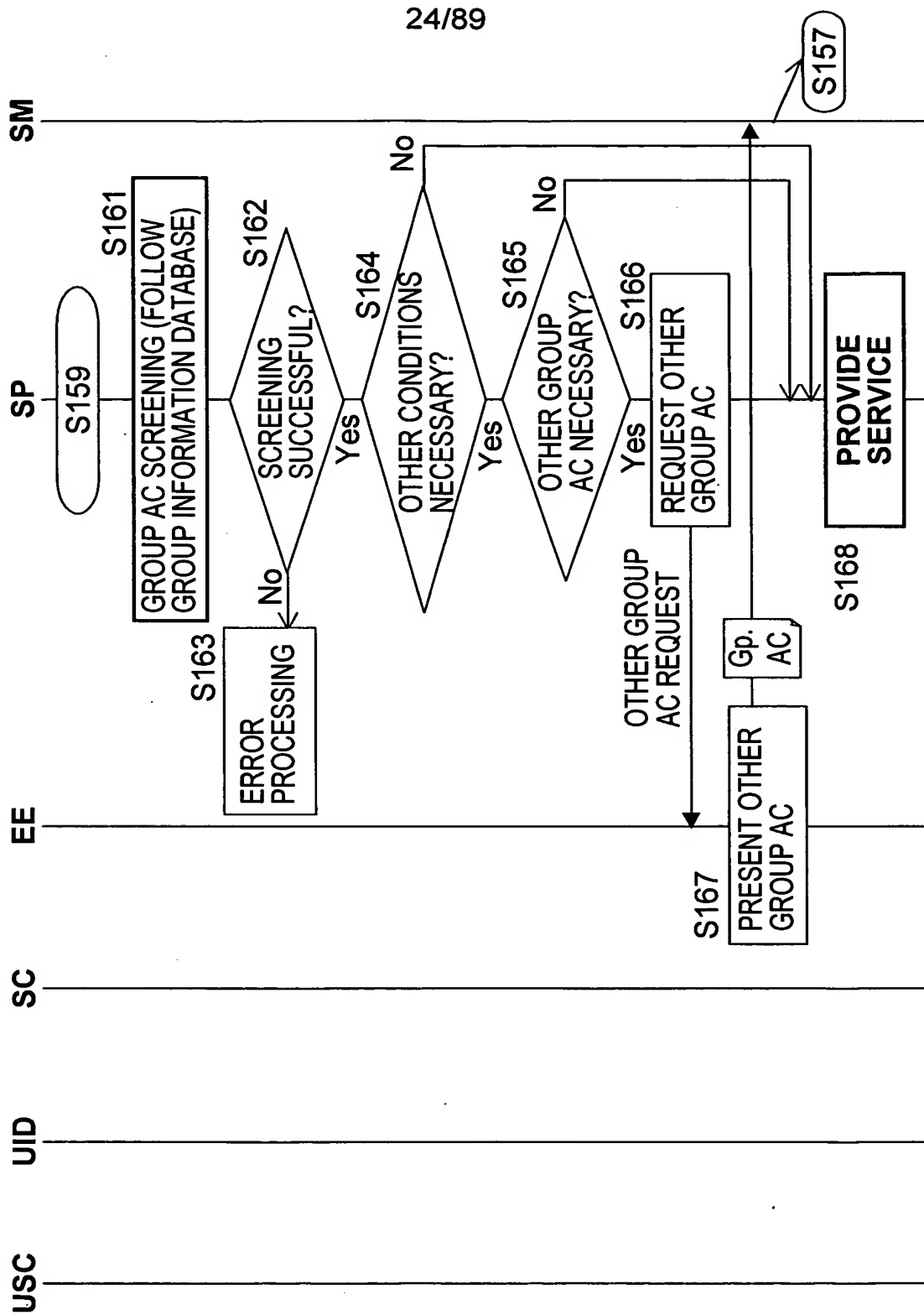
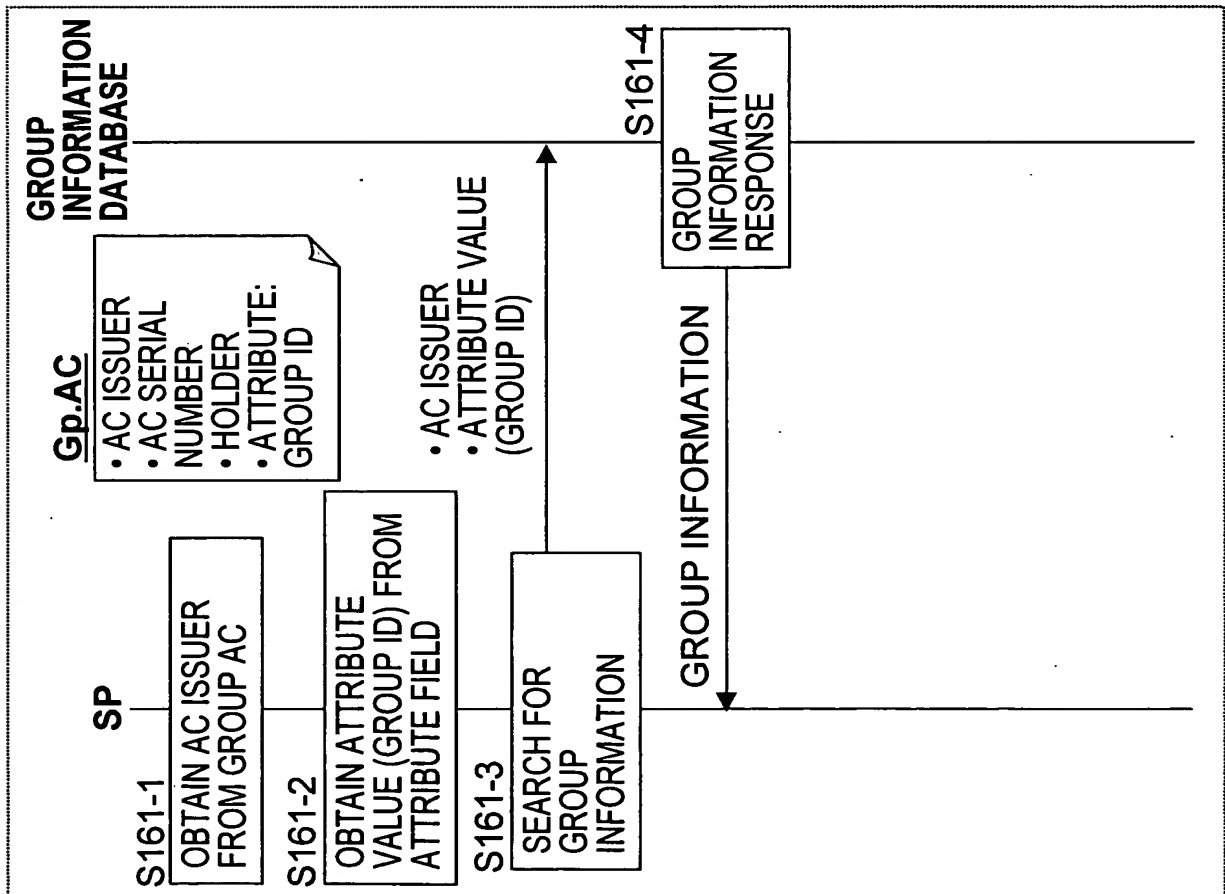


FIG. 24

25/89

FIG. 25



EXAMPLE OF GROUP INFORMATION DATABASE

ISSUER	GROUP ID	GROUP INFORMATION
MANUFACTURER	1001	MAINTENANCE: FULL-SERVICE SUBSCRIBER
MANUFACTURER	1002	MAINTENANCE: TRIAL
GAME DISTRIBUTION SERVICE	1234-0	GAME DISTRIBUTION SERVICE MEMBER
GAME DISTRIBUTION SERVICE	1234-5-10	10-GAME USAGE MEMBER
TANAKA FAMILY, HEAD	001	TANAKA FAMILY, FAMILY
TANAKA FAMILY, HEAD	002	TANAKA FAMILY, CHILDREN

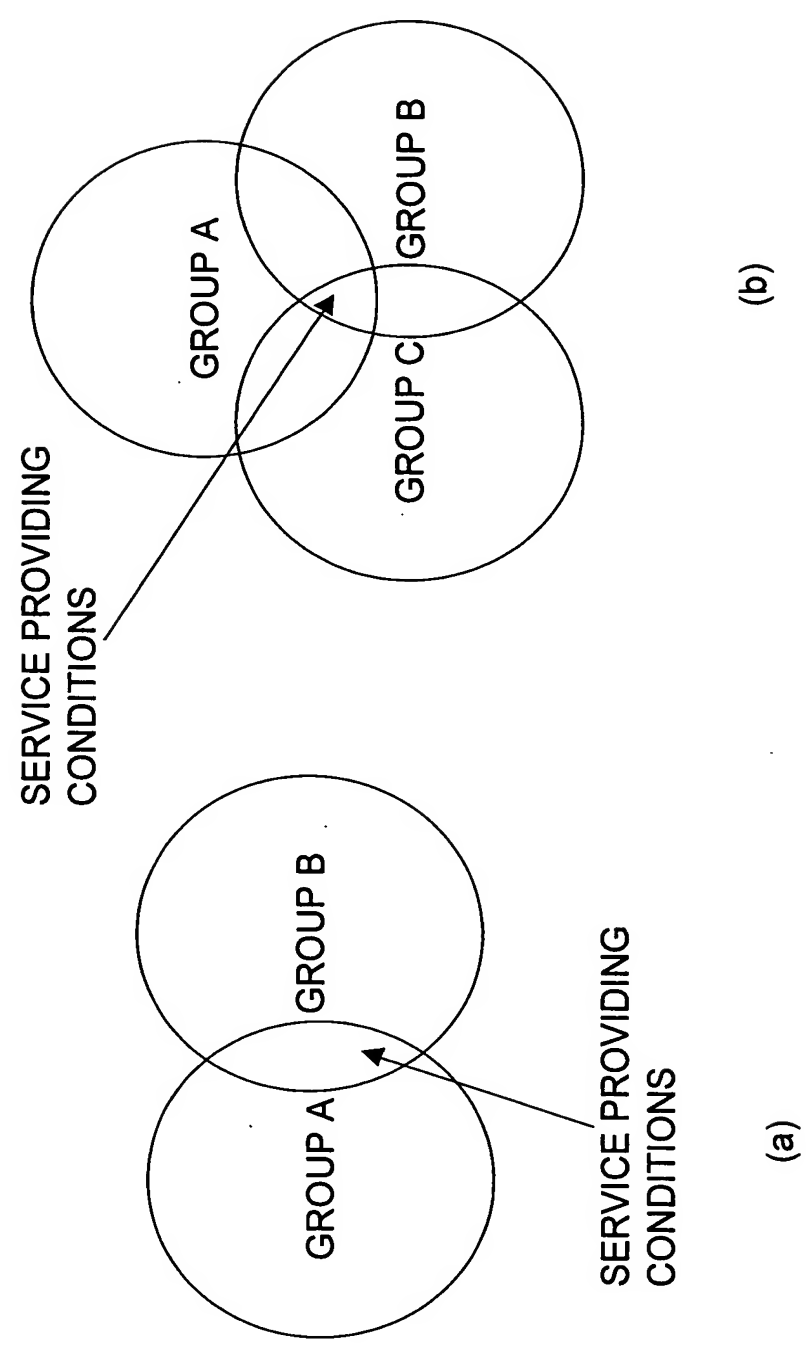


FIG. 26

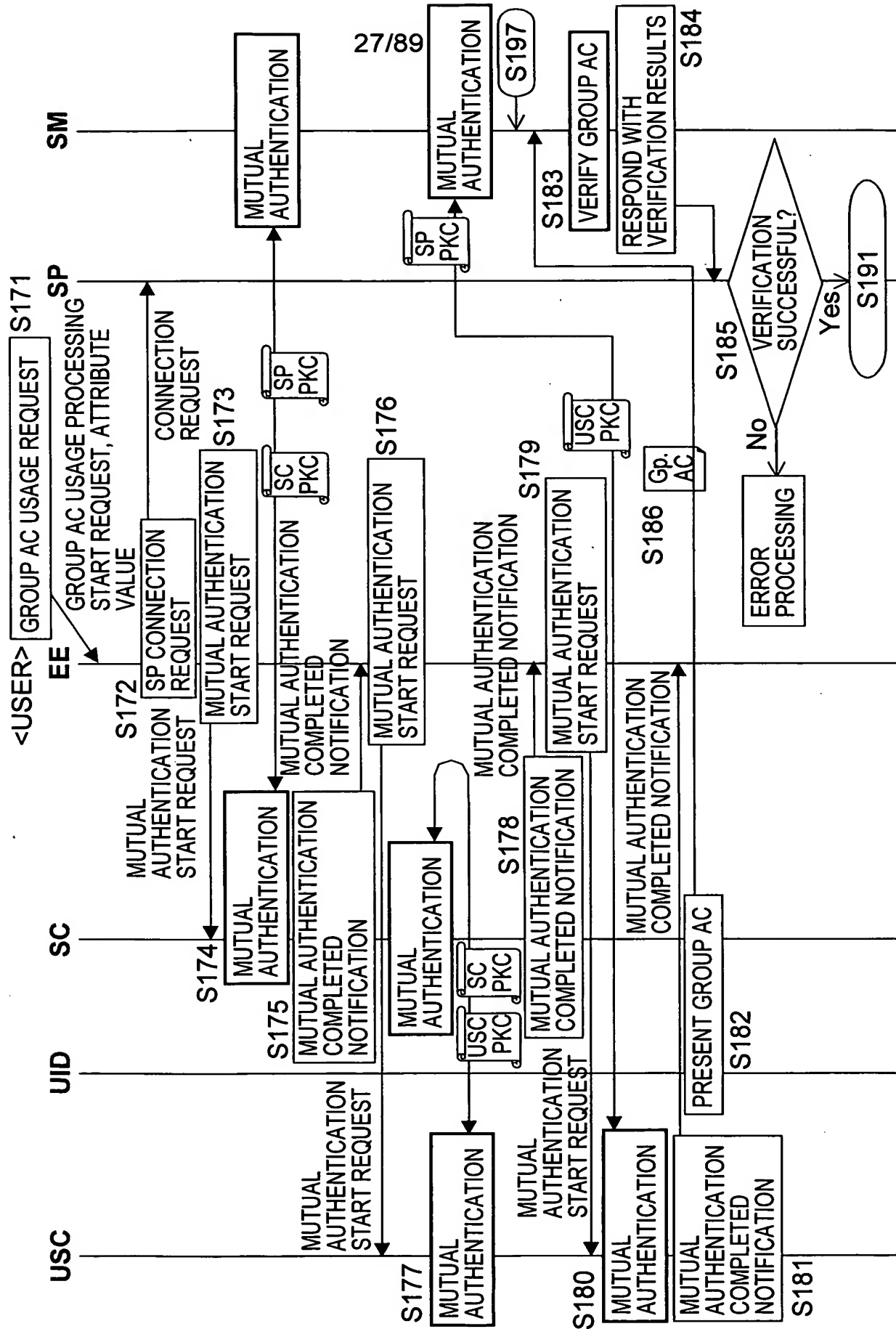


FIG. 27

28/89

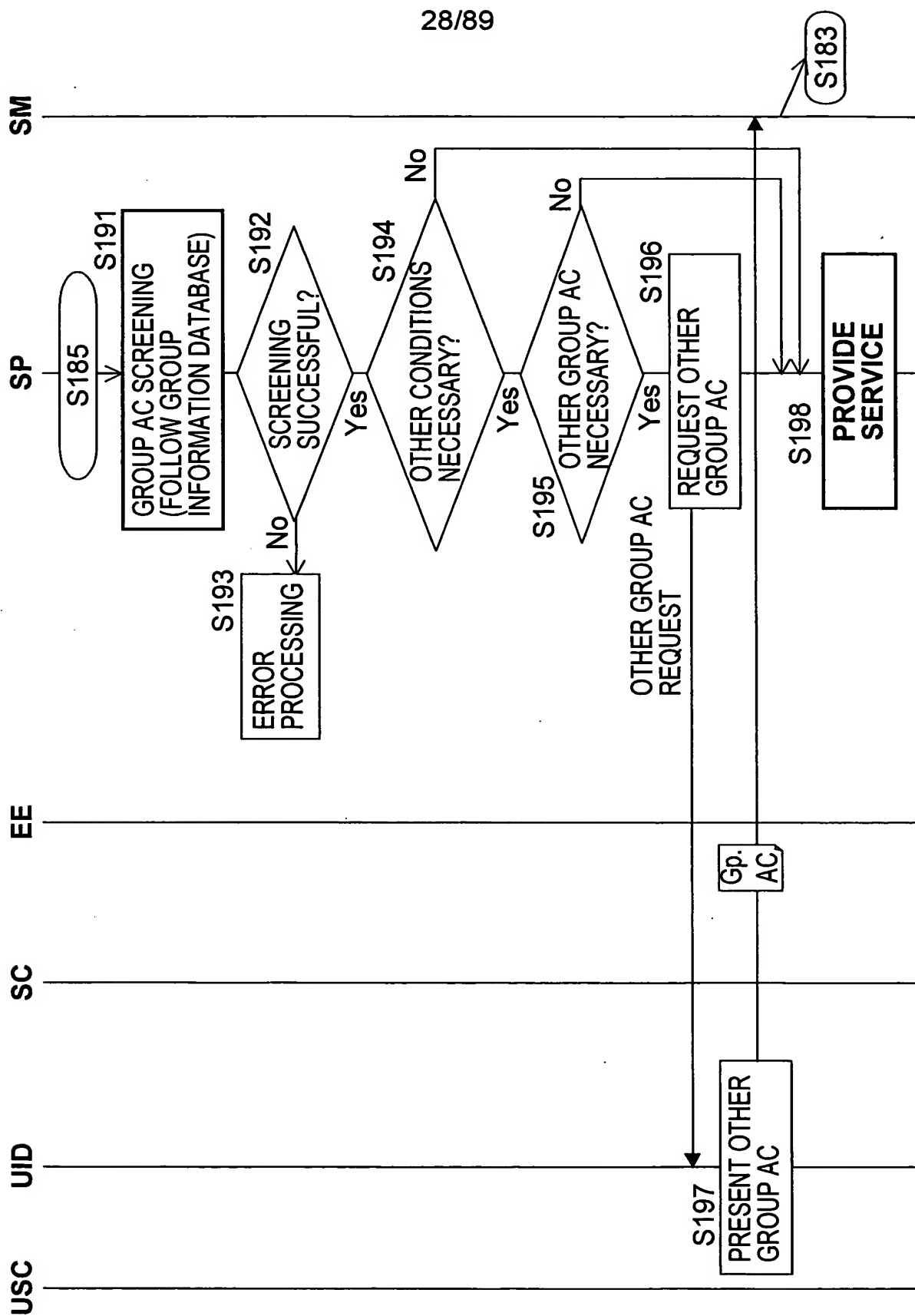
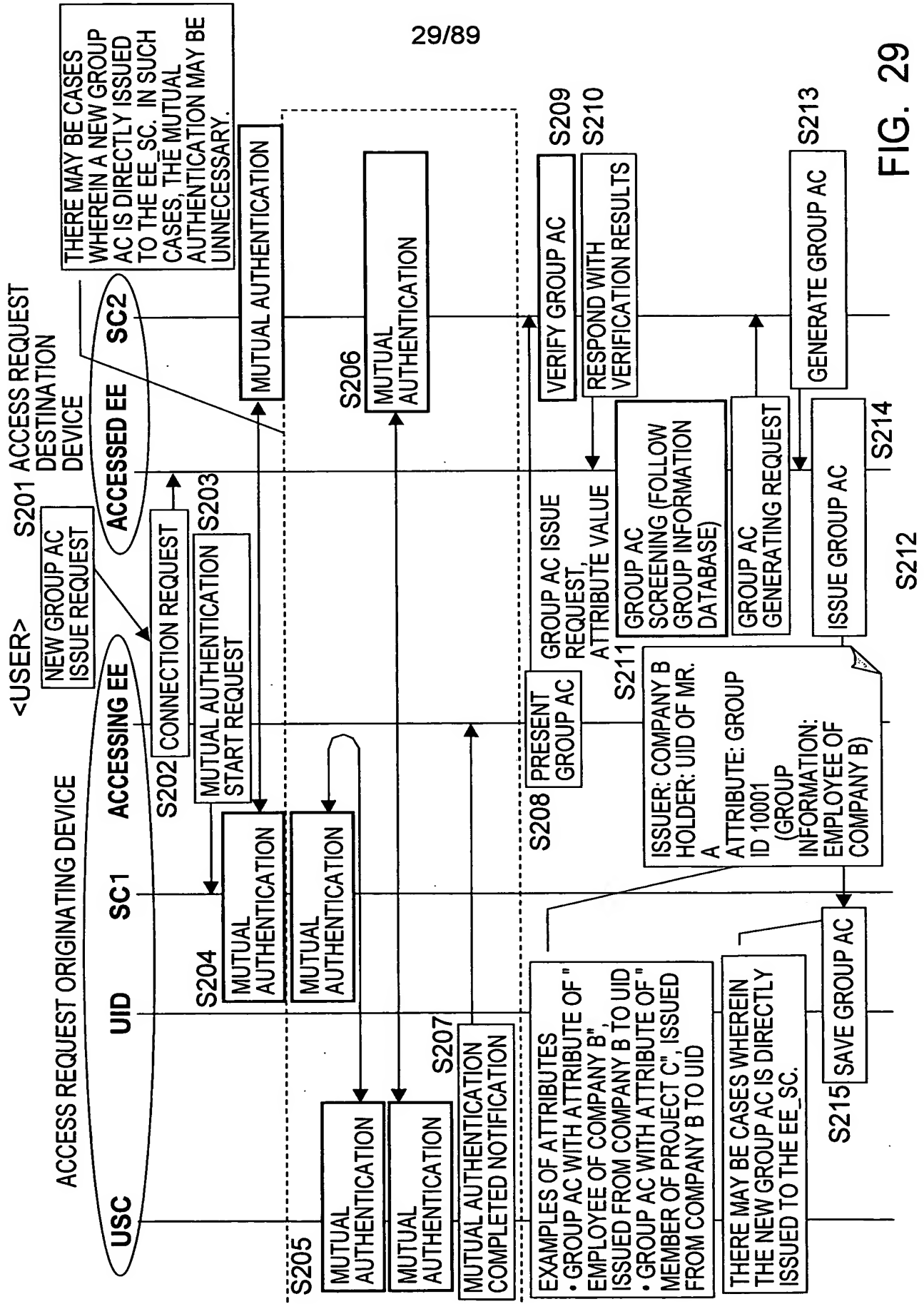


FIG. 28



30/89

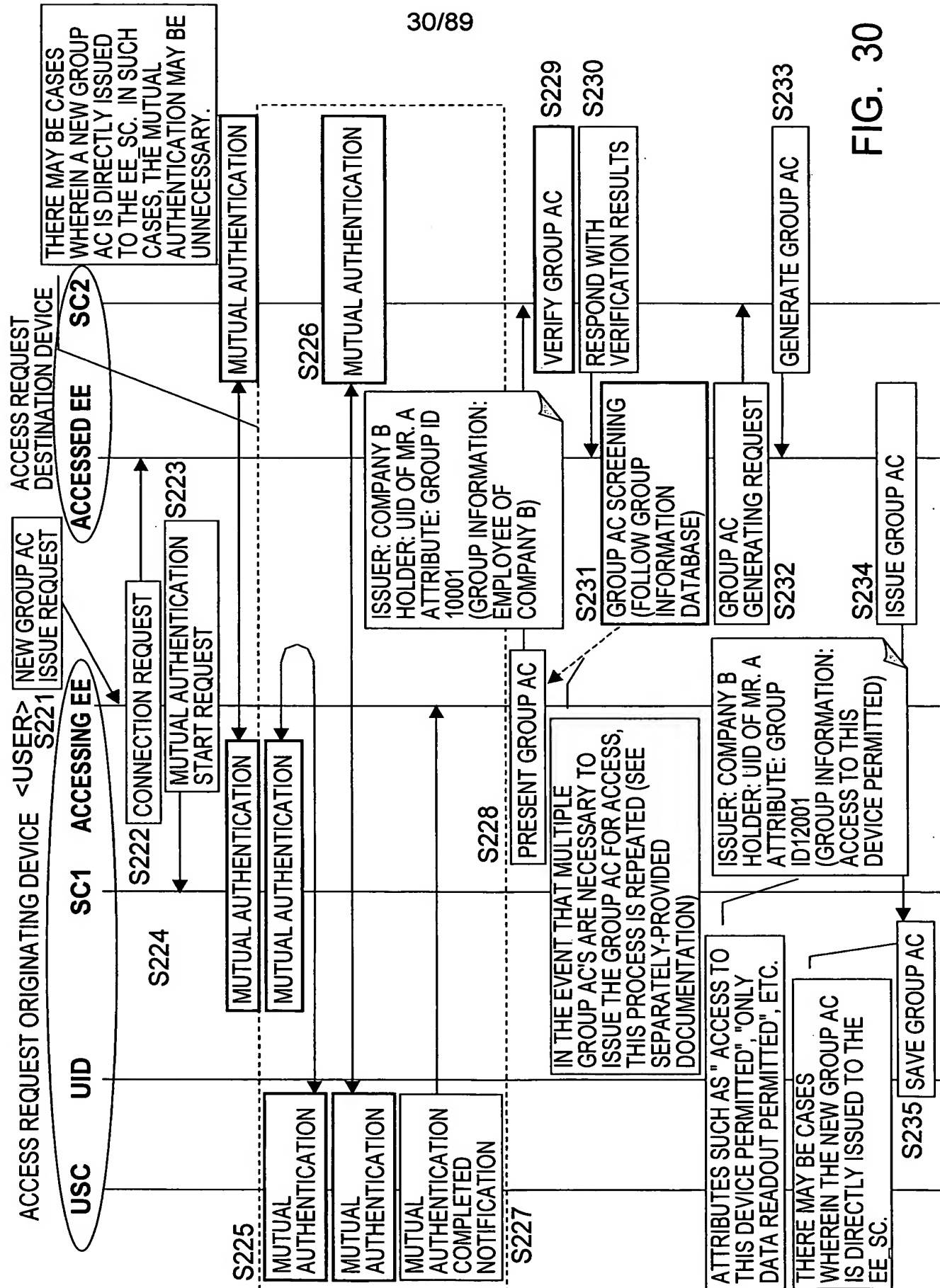


FIG. 30

31/89

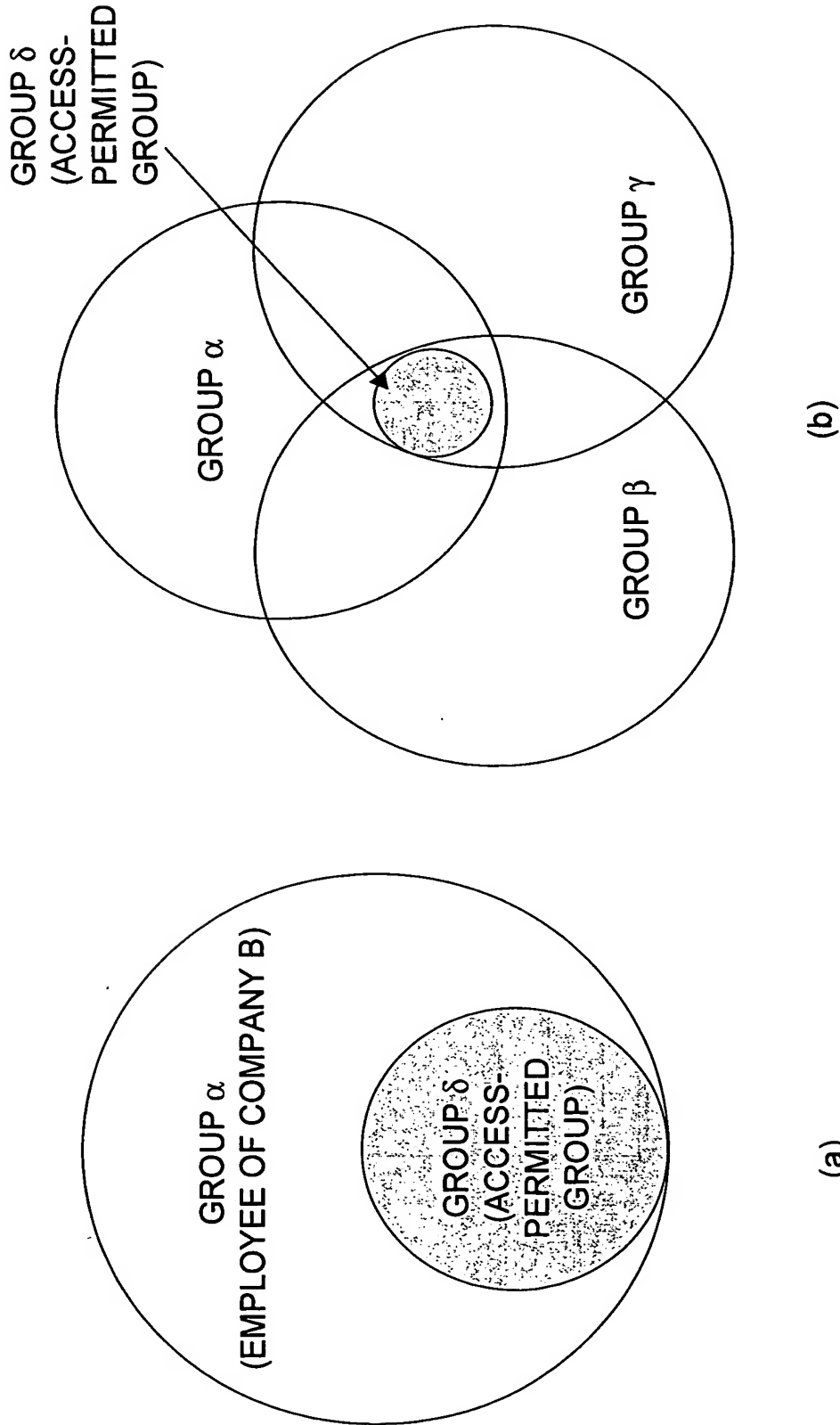
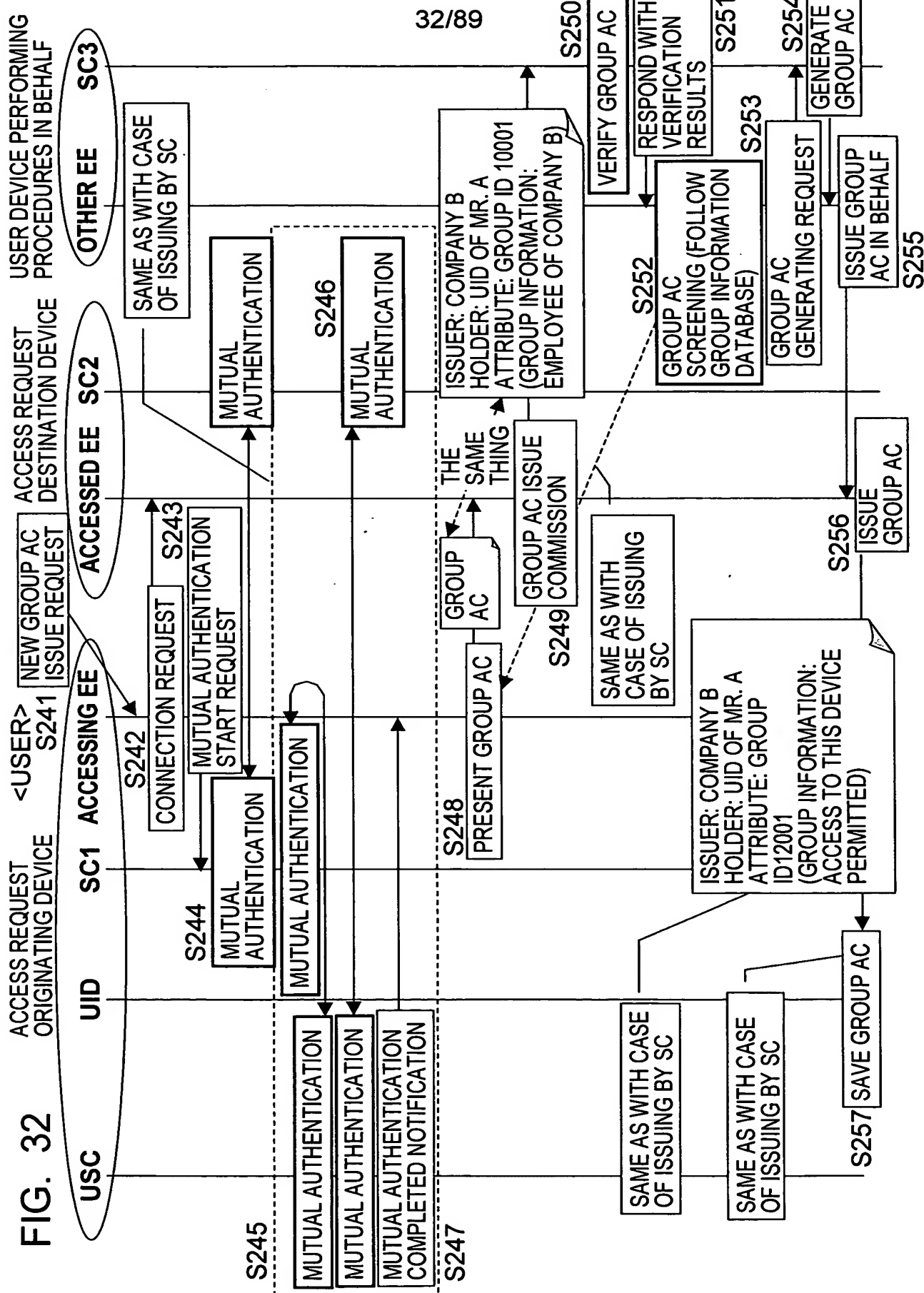


FIG. 31



33/89

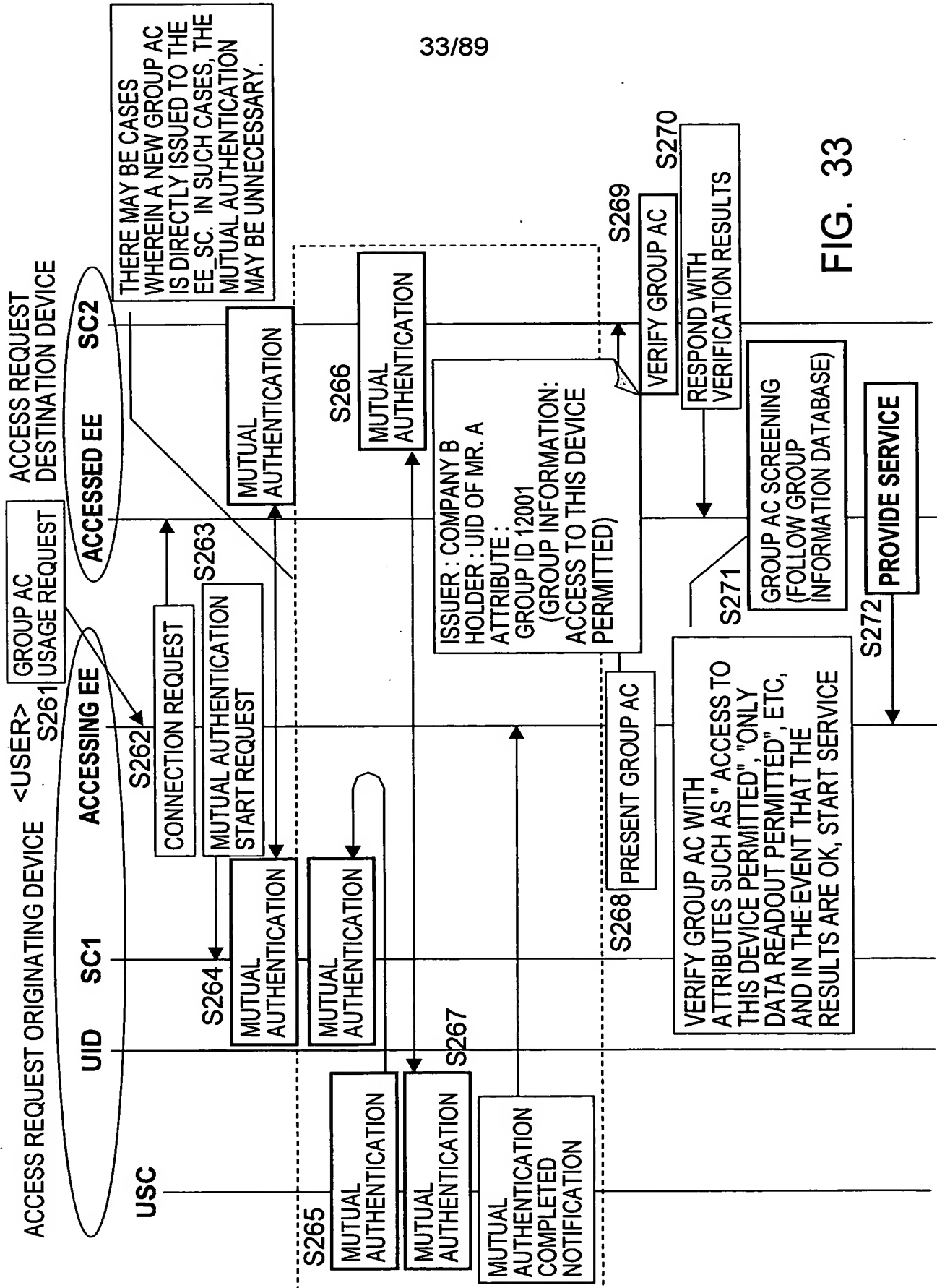


FIG. 33

ISSUER	ISSUING TIMING	HOLDER	VERIFIER	ATTRIBUTE
CARD COMPANY A	OPTIONAL (PERMISSIBLE EVEN BEFORE PURCHASING EE)	MR. A UID_USC	SP_SM	CARD COMPANY A MEMBER
COMPANY B	OPTIONAL (PERMISSIBLE EVEN BEFORE PURCHASING EE)	MR. A UID_USC	SP_SM	EMPLOYEE OF COMPANY B
CITY HALL	OPTIONAL (PERMISSIBLE EVEN BEFORE PURCHASING EE)	INDIVIDUAL FAMILY MEMBER UID_USC	SP_SM	FAMILY OF MR. A
MR. A	OPTIONAL (PERMISSIBLE EVEN BEFORE PURCHASING EE)	INDIVIDUAL FAMILY MEMBER UID_USC	SP_SM	FAMILY OF MR. A
EE MANUFACTURER C	AT TIME OF PURCHASING EE	MR. A UID_USC	SP_SM	USER REGISTRATION FOR EE
EE MANUFACTURER C	AT TIME OF MANUFACTURING EE	DEVICE EE_SC	SP_SM	EE REGISTRATION FOR EE
MR. A	AFTER PURCHASING EE	DEVICE EE_SC	SP_SM	OWNED BY ISSUER
EE MANUFACTURER C	AFTER PURCHASING EE	DEVICE EE_SC	SP_SM	DEVICE OF MR. A

FIG. 34

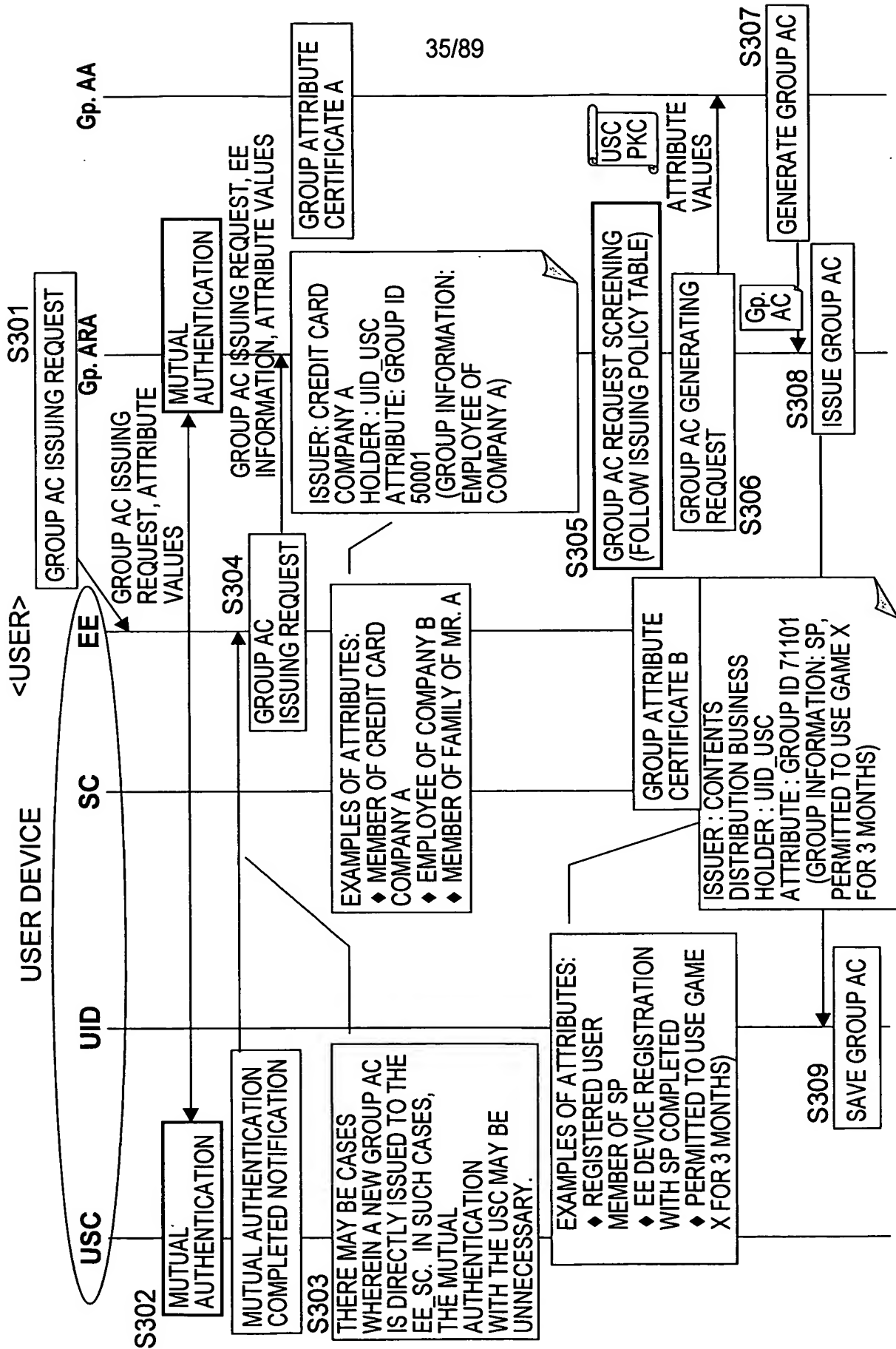


FIG. 35

36/89

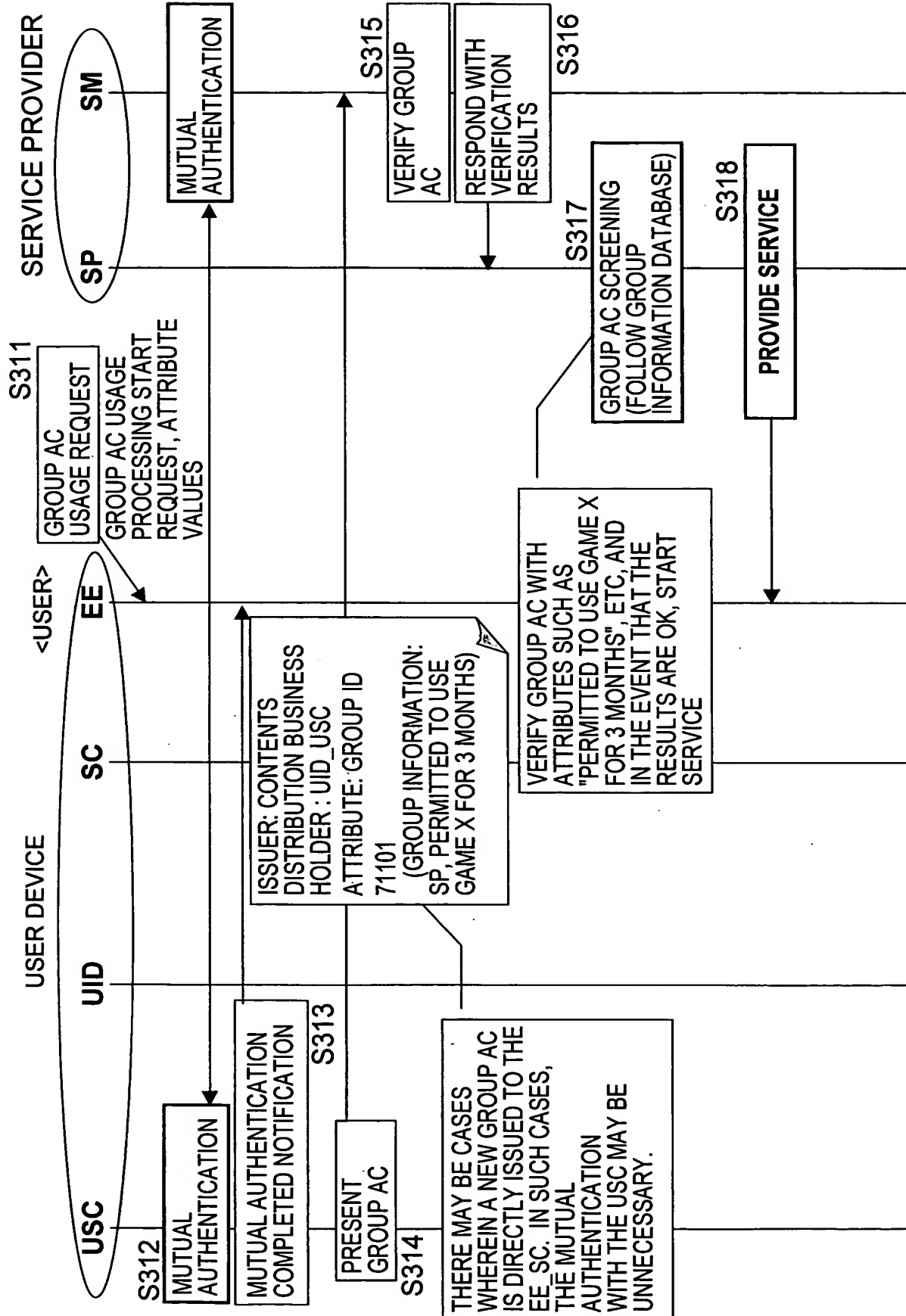


FIG. 36

	AC TITLE	ATTRIBUTE INFORMATION (= ISSUING POLICY)	ISSUER (GROUP AA, ARA)	HOLDER
AC01	1. STUDENT ID CARD	STUDENT OF ISSUER	UNIVERSITY A (AA OPERATED (MANAGED) THEREBY)	USC OF UID OF USER C
AC02	2. ART CLASS PARTICIPANT CARD	HOLDER OF RIGHT TO PARTICIPATE IN ART CLASSES HOSTED BY ISSUER	UNIVERSITY A (AA OPERATED (MANAGED) THEREBY)	USC OF UID OF USER C
AC03	3. MANAGED DEVICE CERTIFICATE	DEVICE MANAGED BY ISSUER	UNIVERSITY A (AA OPERATED (MANAGED) THEREBY)	SC OF TELEVISION D WHICH IS AN END ENTITY (EE)
AC04	4. EDUCATIONAL DEVICE CERTIFICATE	DEVICE FOR EDUCATIONAL USE	MINISTRY OF EDUCATION, CULTURE, SPORTS, SCIENCE AND TECHNOLOGY (AA OPERATED (MANAGED) THEREBY)	SC OF TELEVISION D WHICH IS AN END ENTITY (EE)

FIG. 37

38/89

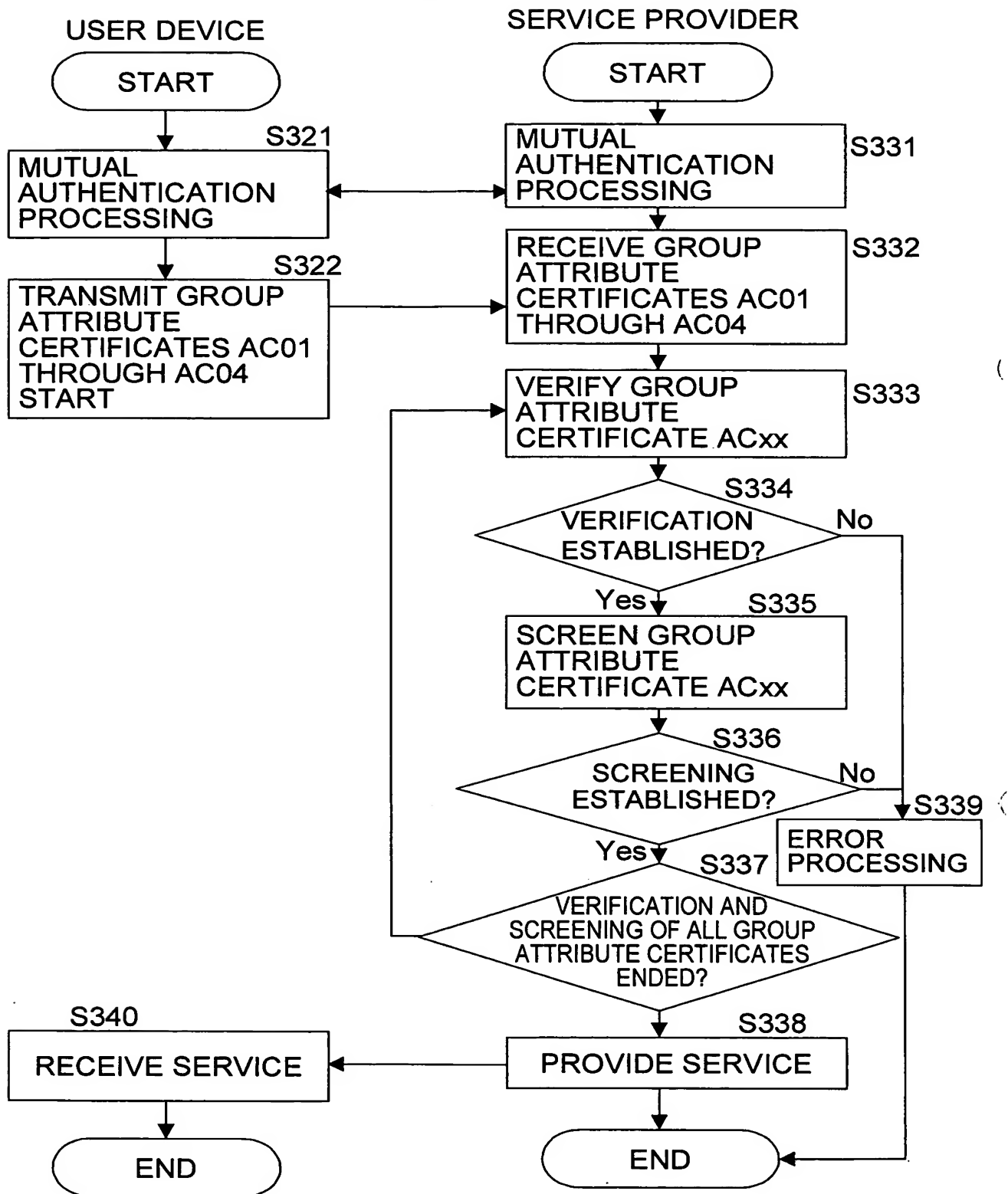


FIG. 38

SERVICE	AC ISSUER, AC	...	AC ISSUER, AC	INFORMATION OTHER THAN AC	...
VIEW/LISTEN CONTENTS B	UNIVERSITY A, STUDENT IDENTIFICATION CARD		MINISTRY OF EDUCATION, CULTURE, SPORTS, SCIENCE AND TECHNOLOGY, EDUCATIONAL DEVICE CERTIFICATE		
VIEW/LISTEN CONTENTS B					
...					
VIEW/LISTEN CONTENTS G					

FIG. 39

40/89

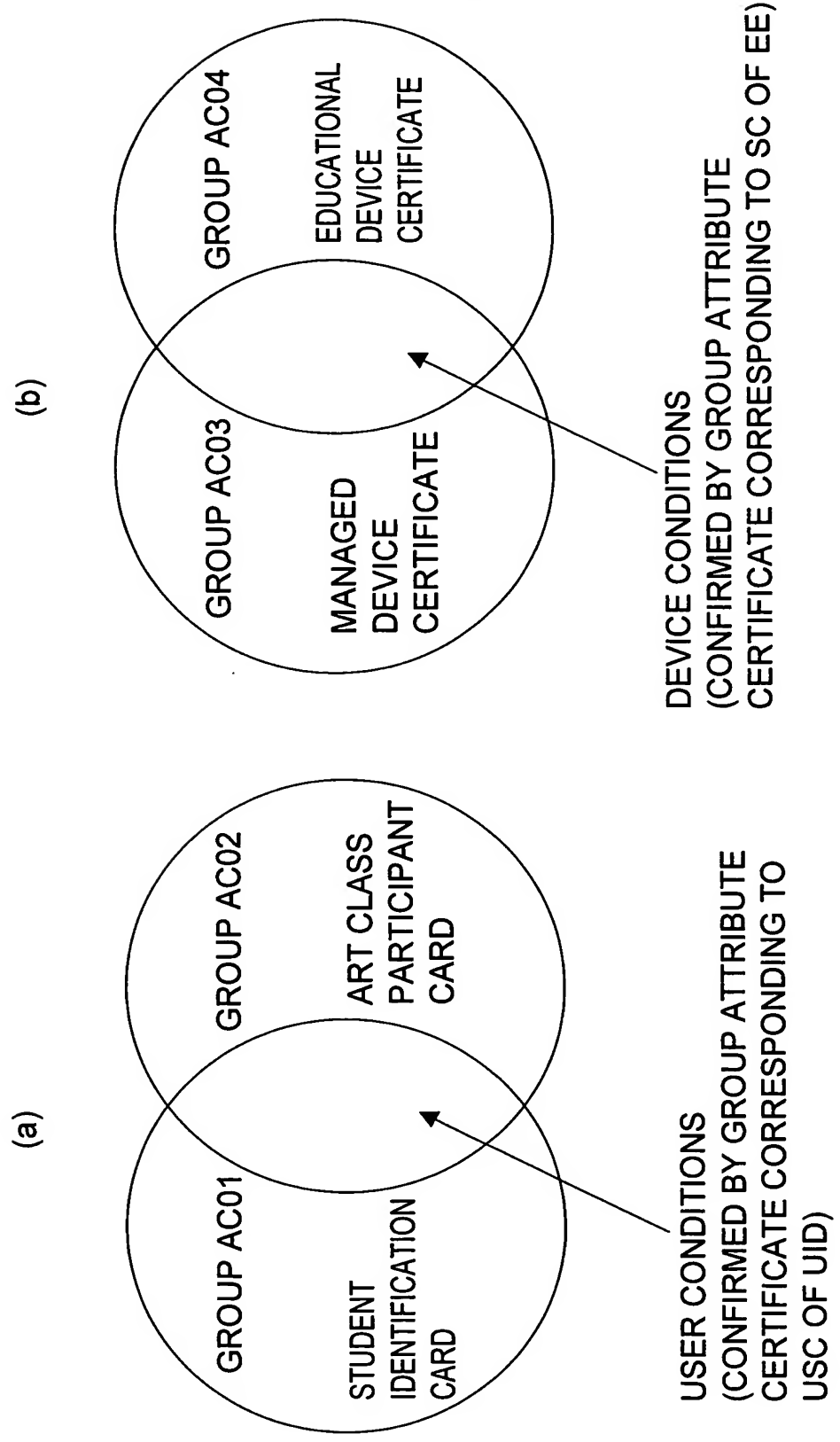


FIG. 40

	ISSUER	HOLDER	VERIFIER	ATTRIBUTE
AC01	HOSPITAL SIDE MEDICAL DEVICE (SP)	UID_USC OR EE_SC OF MR. A	HOSPITAL SIDE MEDICAL DEVICE (SP_SM)	PERMITTED TO RUN PROGRAM E
AC02	HOME SIDE MEDICAL DEVICE (EE)	HOSPITAL SIDE MEDICAL DEVICE (SP_SM)	HOME SIDE MEDICAL DEVICE (EE_SC)	PERMITTED TO HANDLE DATA X

FIG. 41

42/89

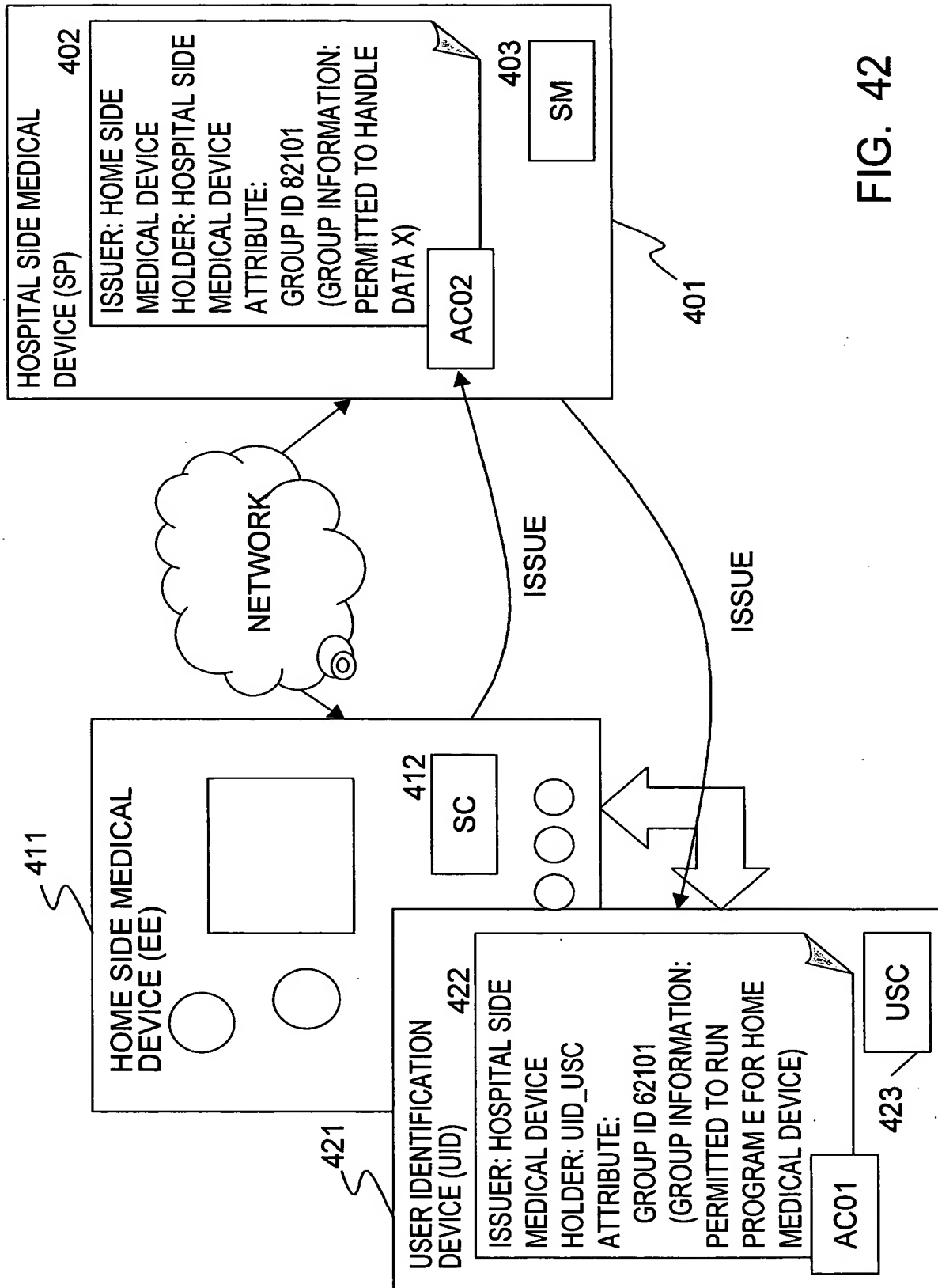
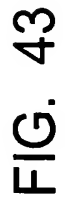
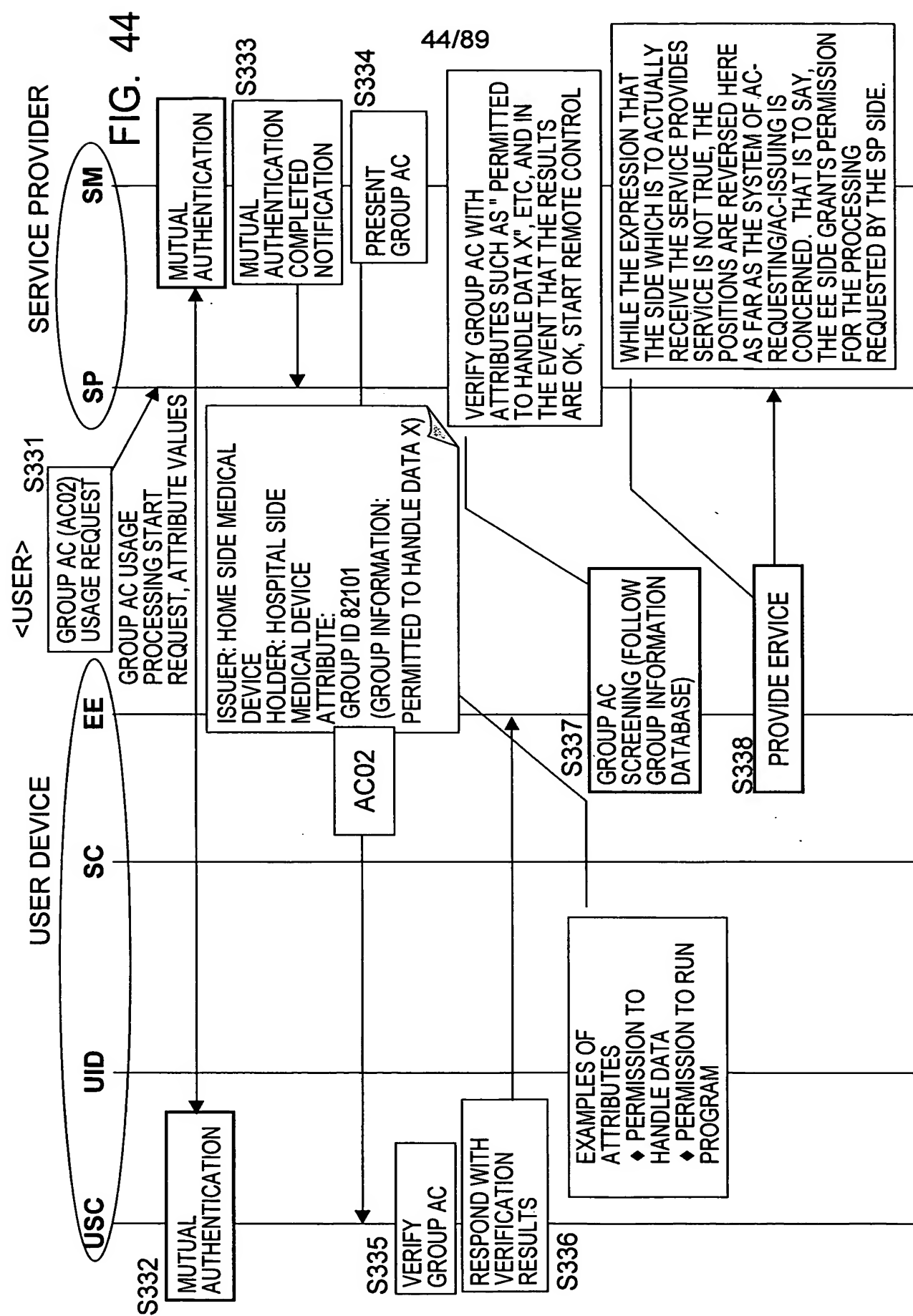


FIG. 42





	ISSUER	ISSUING TIMING	HOLDER	VERIFIER	ATTRIBUTE
SERVICE AC	HOME APPLIANCE MANUFACTURER (SP)	AT TIME OF PURCHASING HOME APPLIANCE	MR. A UID_USC or EE_SC	SP_SM	EE MAINTENANCE SERVICE CONTENTS
CONTROL AC	HOME APPLIANCE (EE)	PRIOR TO OR AT TIME OF AUTOMATIC MAINTENANCE	SP_SM	EE_SC	HOME APPLIANCE CONTROL CONSTRAINT RANGE X

FIG. 45

46/89

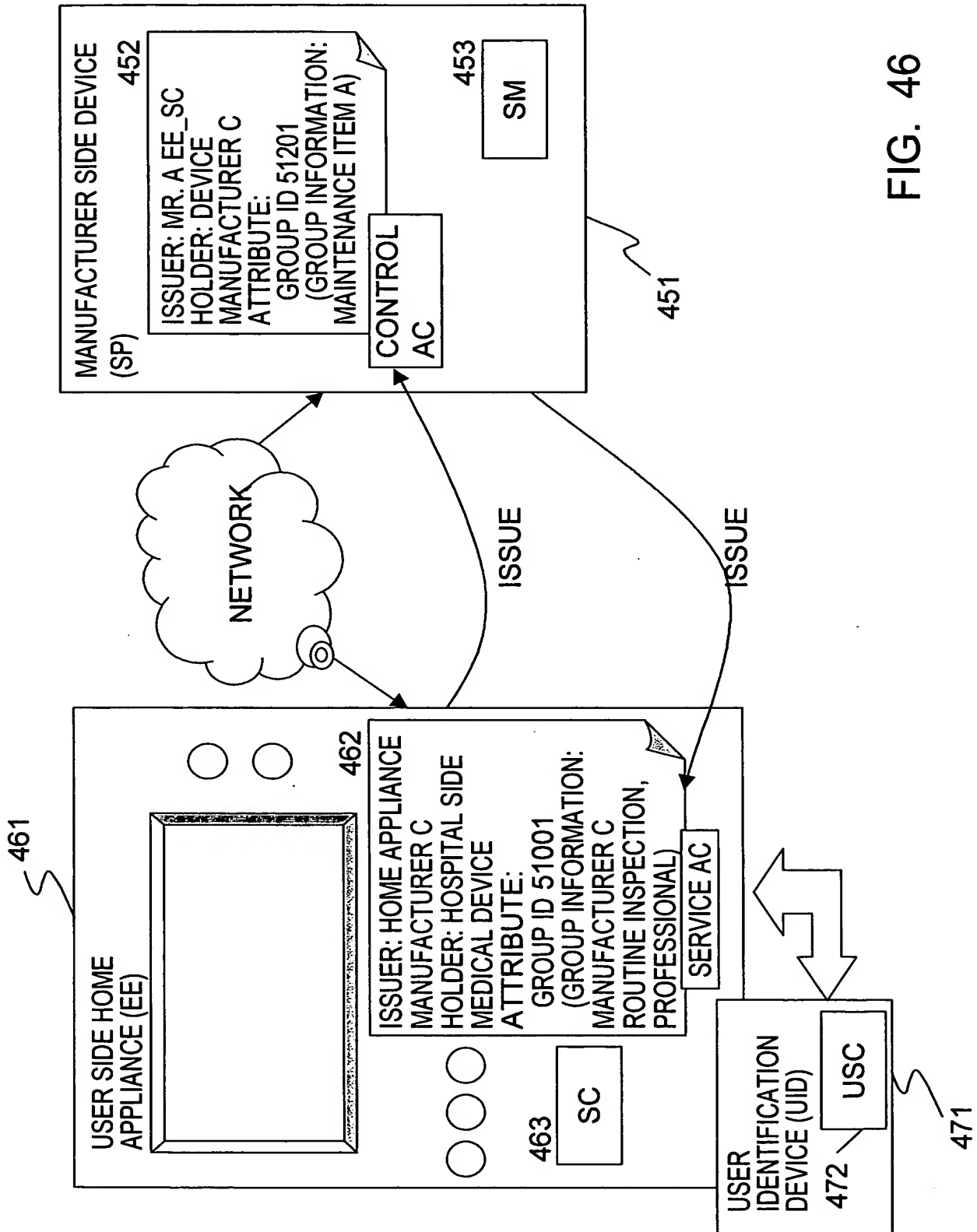


FIG. 46

47/89

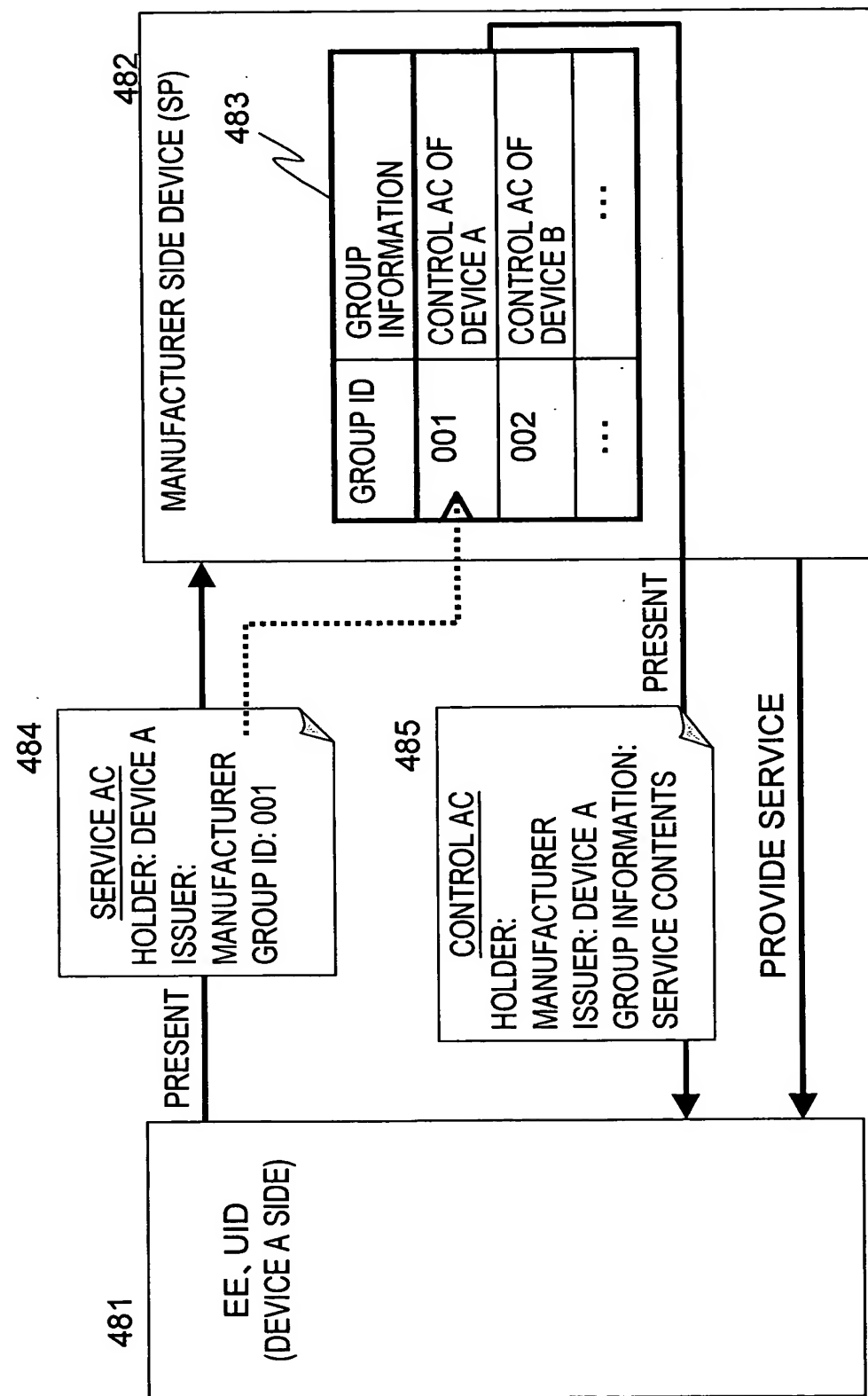
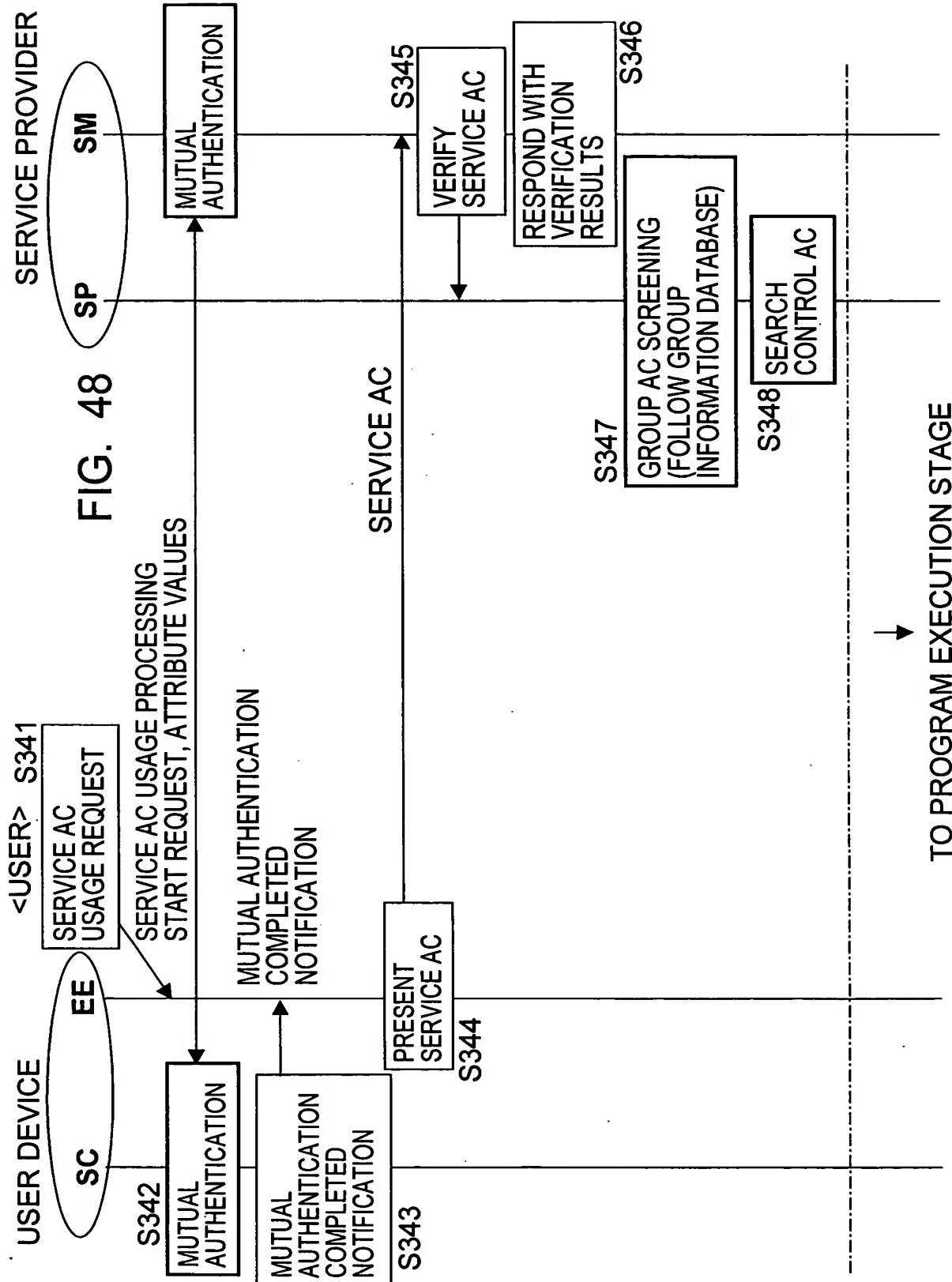


FIG. 47

48/89



49/89

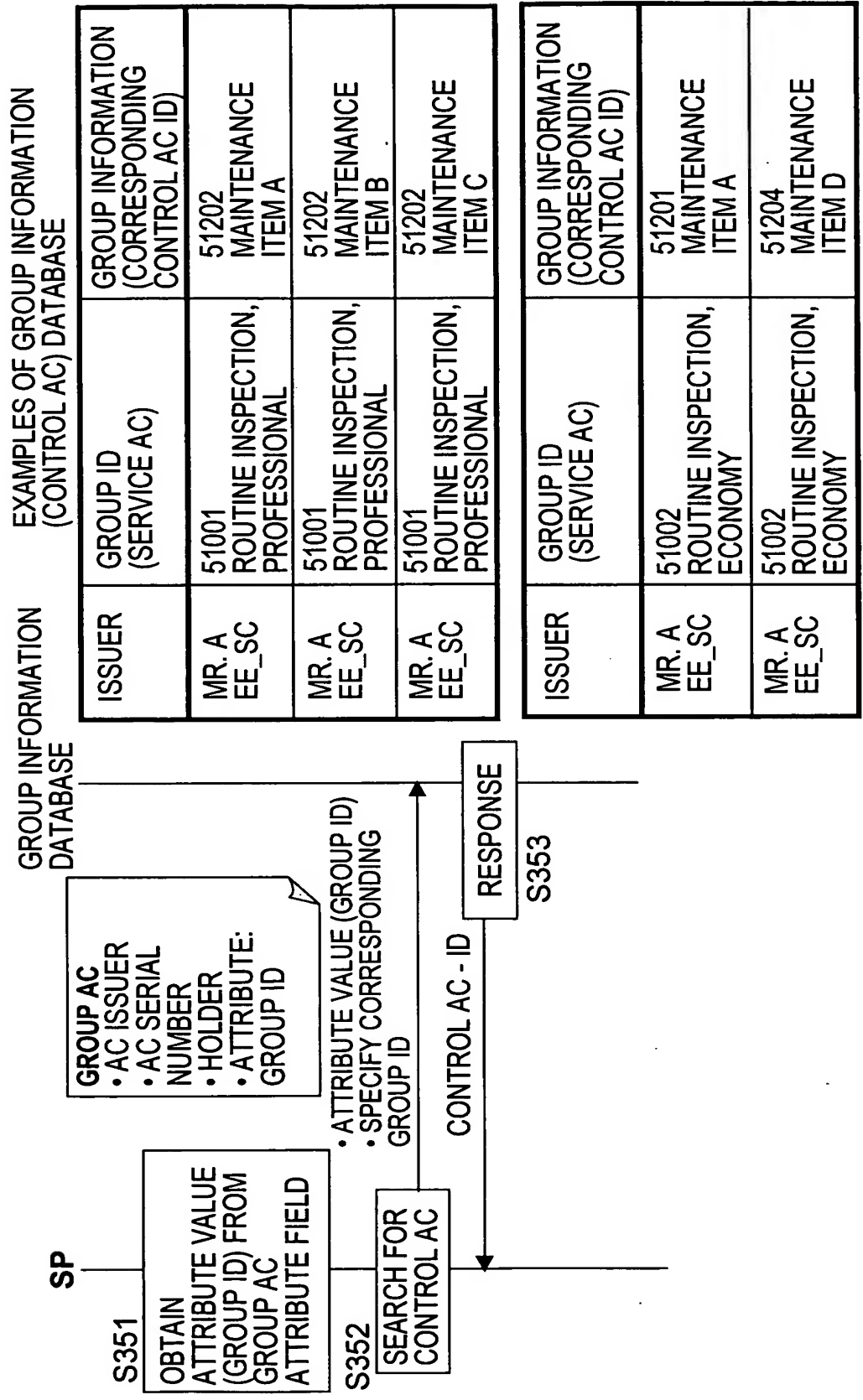
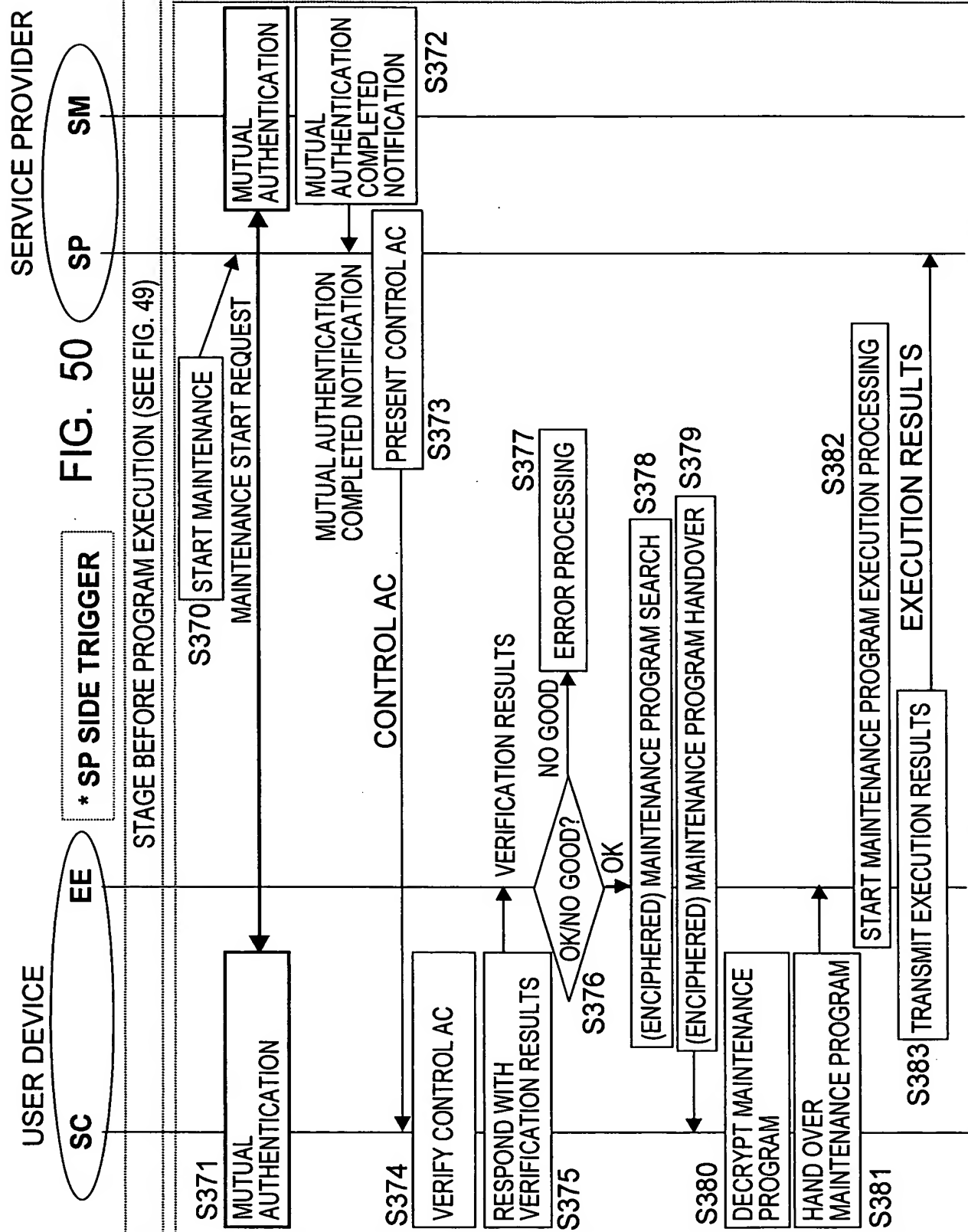
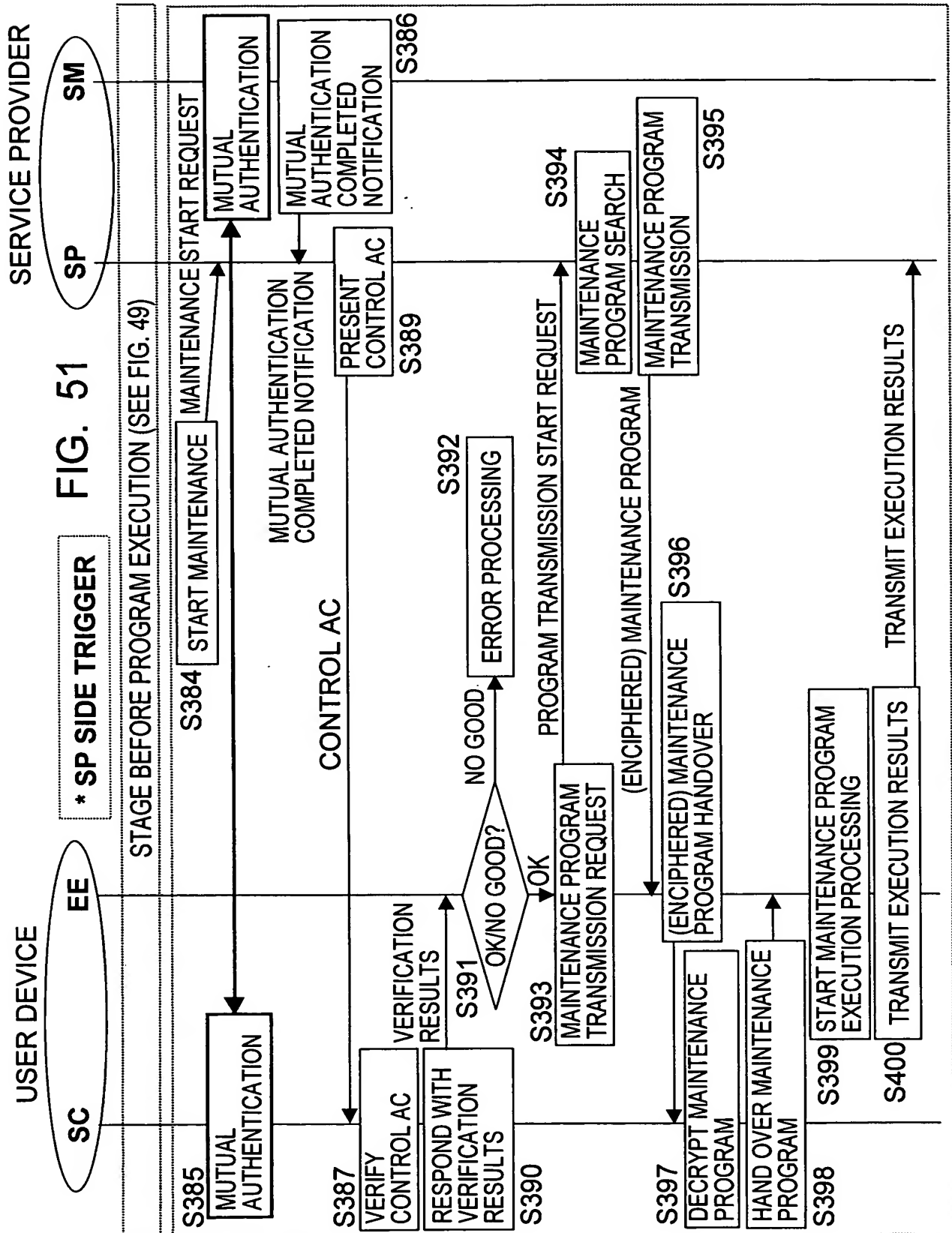


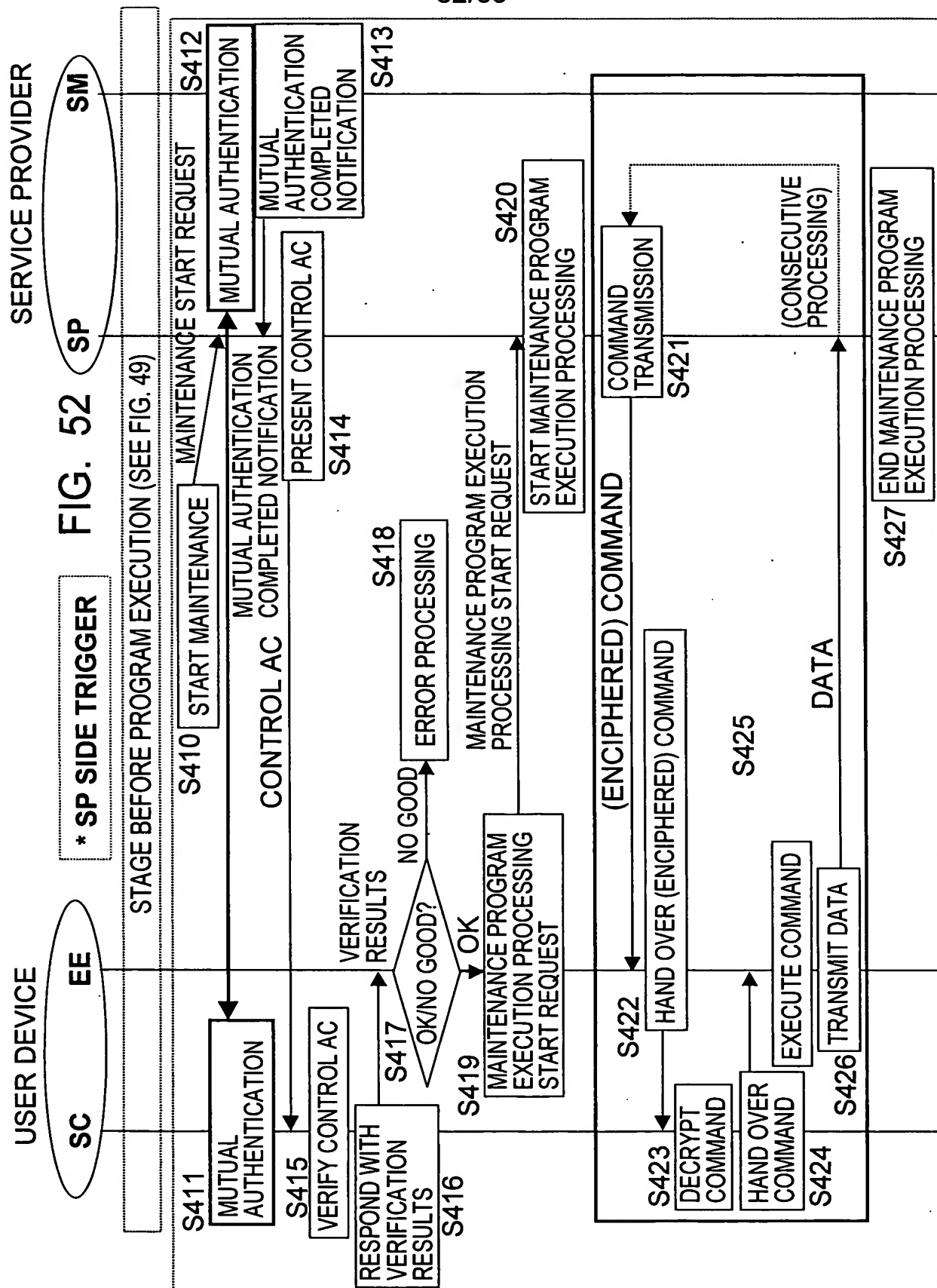
FIG. 49

50/89



51/89





53/89

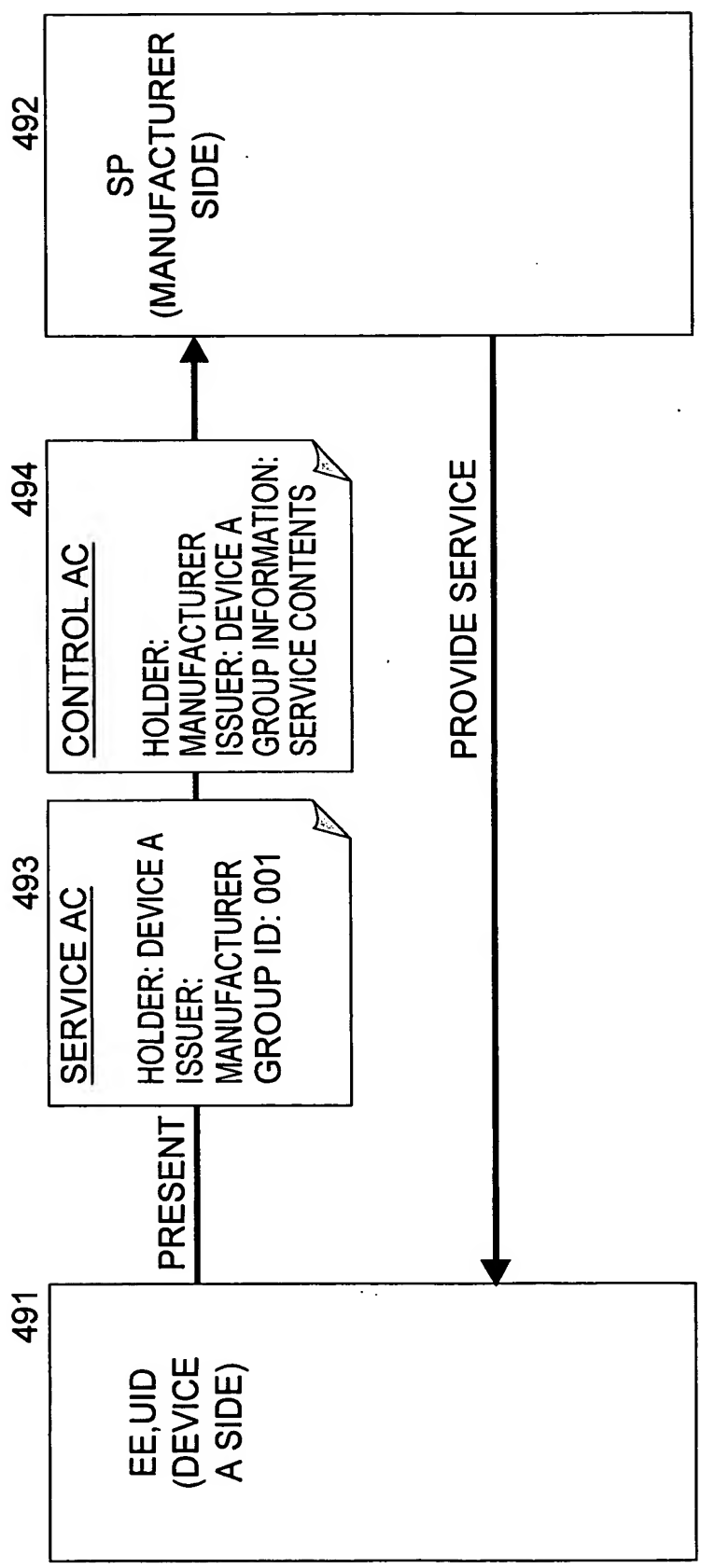


FIG. 53

	ISSUER	ISSUING TIMING	HOLDER	VERIFIER	ATTRIBUTE
AC01	CHAT ADMINISTRATOR (SP)	AT LOGIN	MR. A UID_USC or EE_SC	SP_SM	SP SERVER ACCESS PRIVILEGES
AC02	MR. B (SP)	AT LOGIN	MR. A UID_USC or EE_SC	MR. B UID_USC or EE_SC	MR. B SERVER ACCESS PRIVILEGES

FIG. 54

55/89

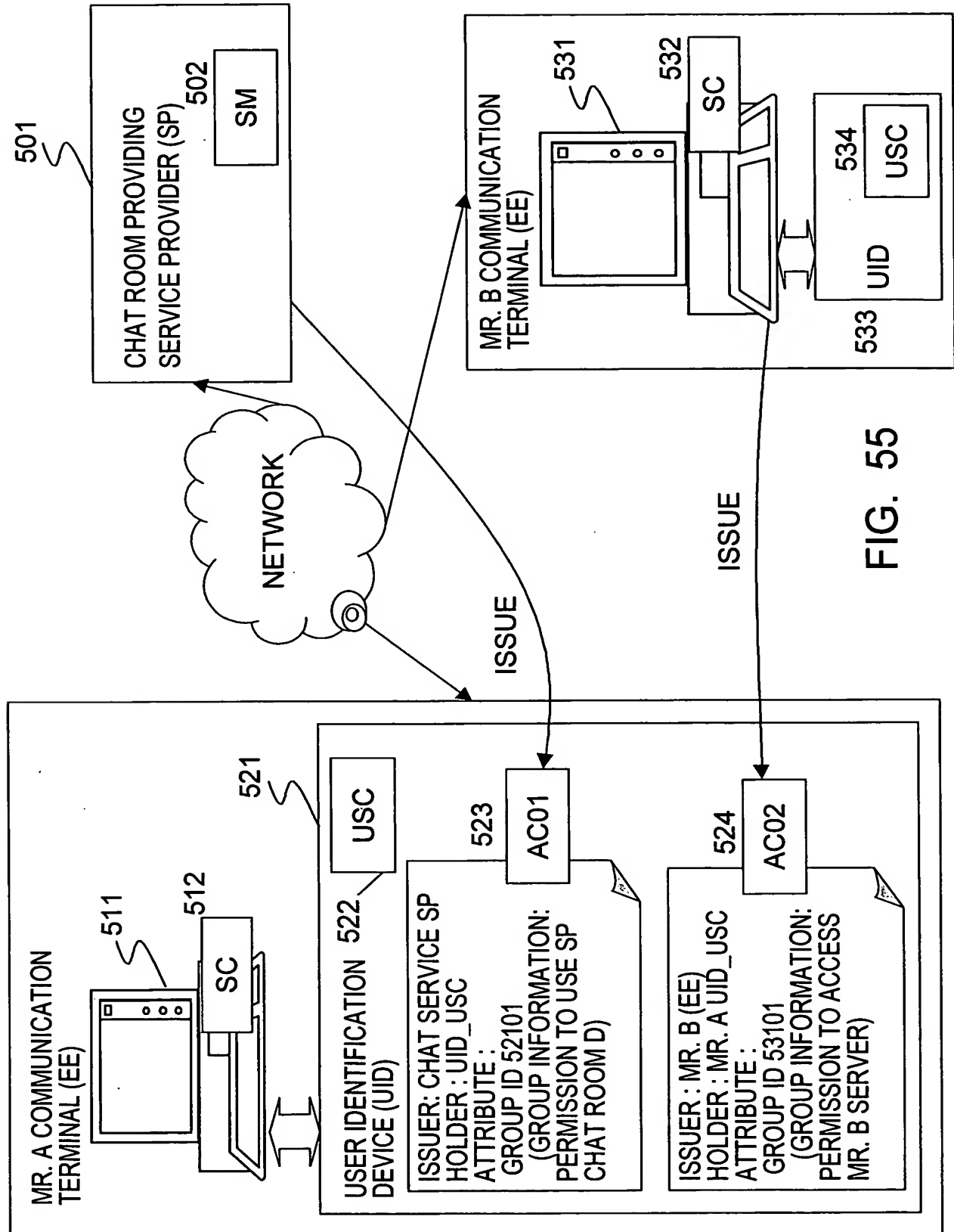


FIG. 55

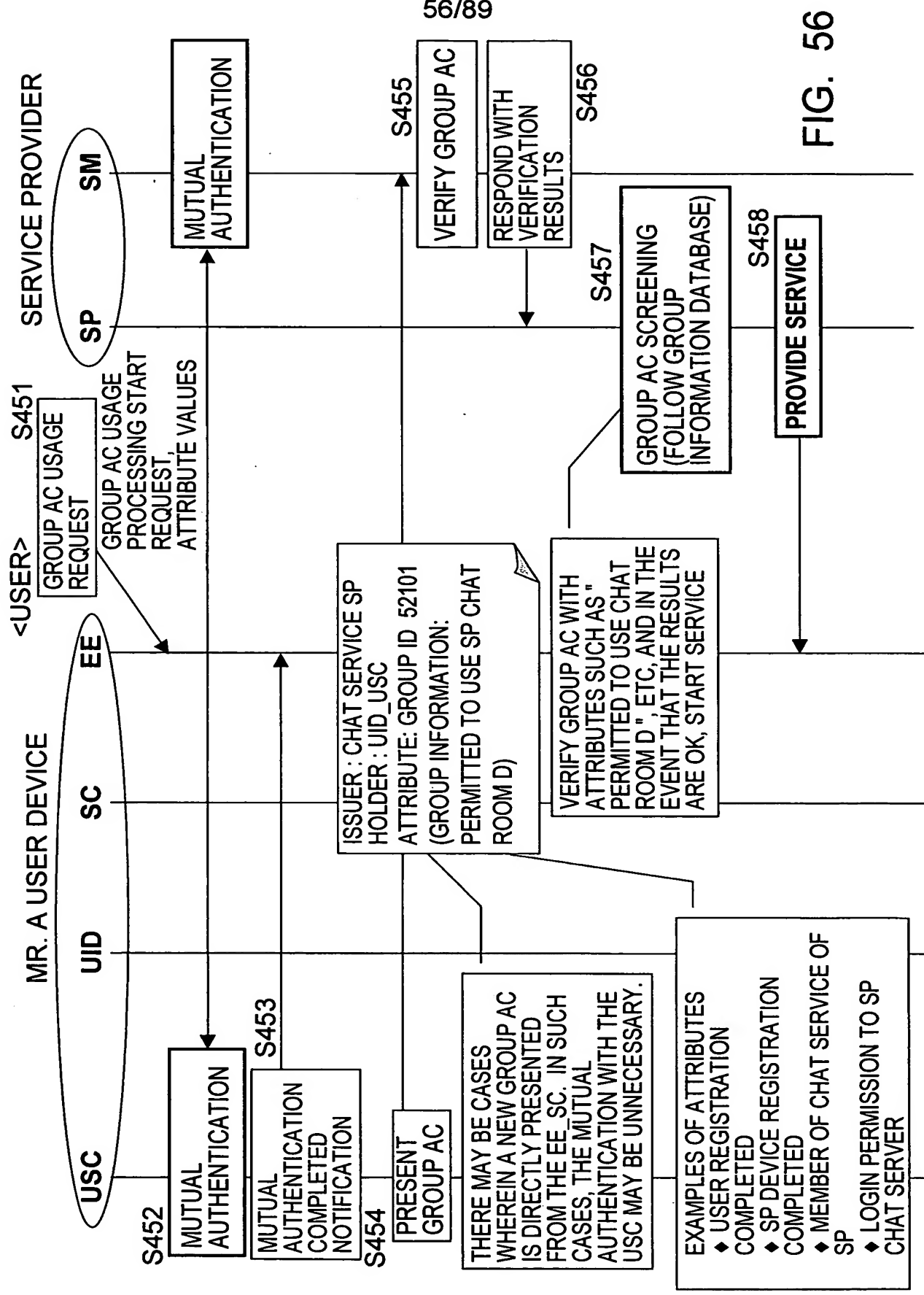
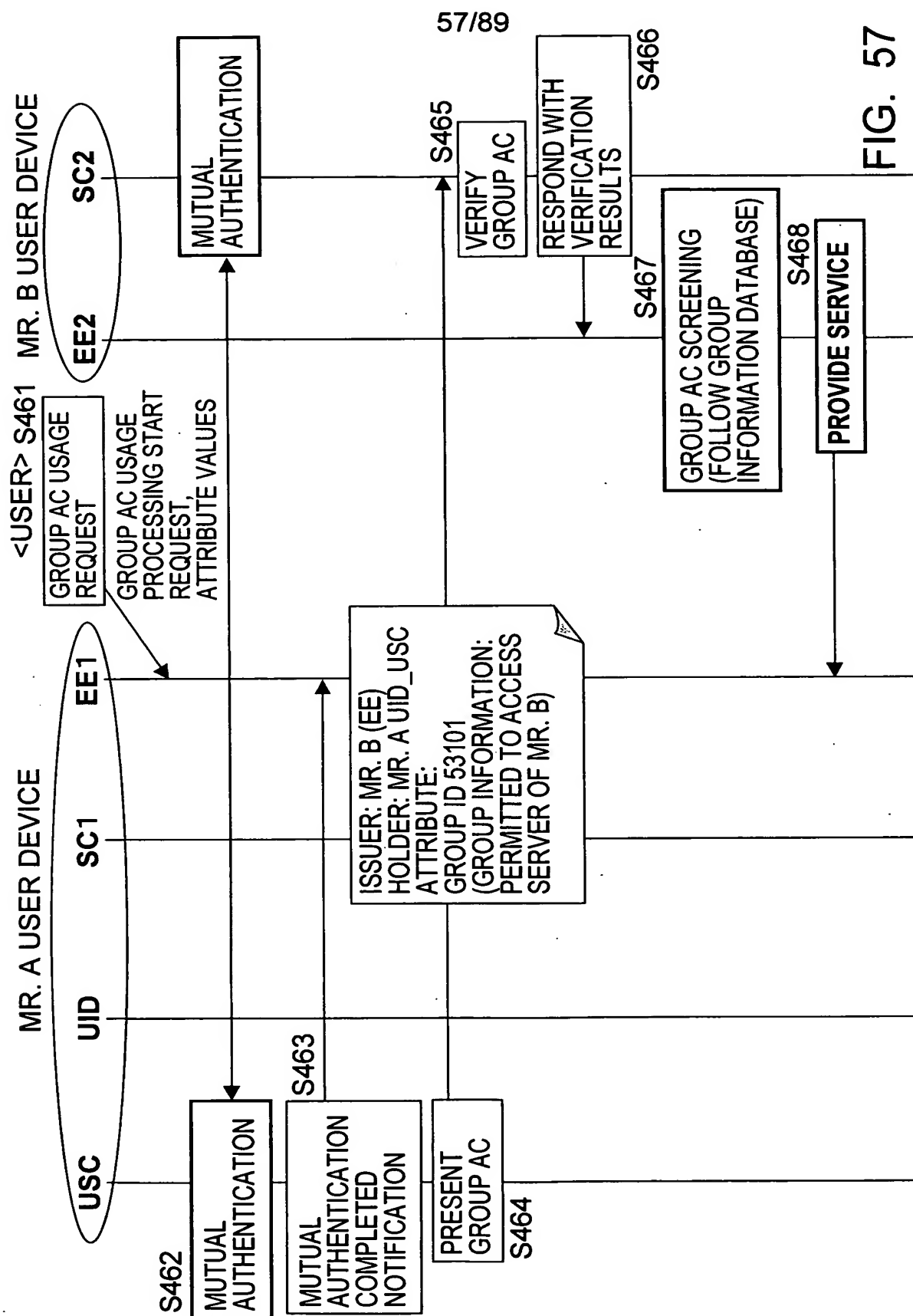


FIG. 56



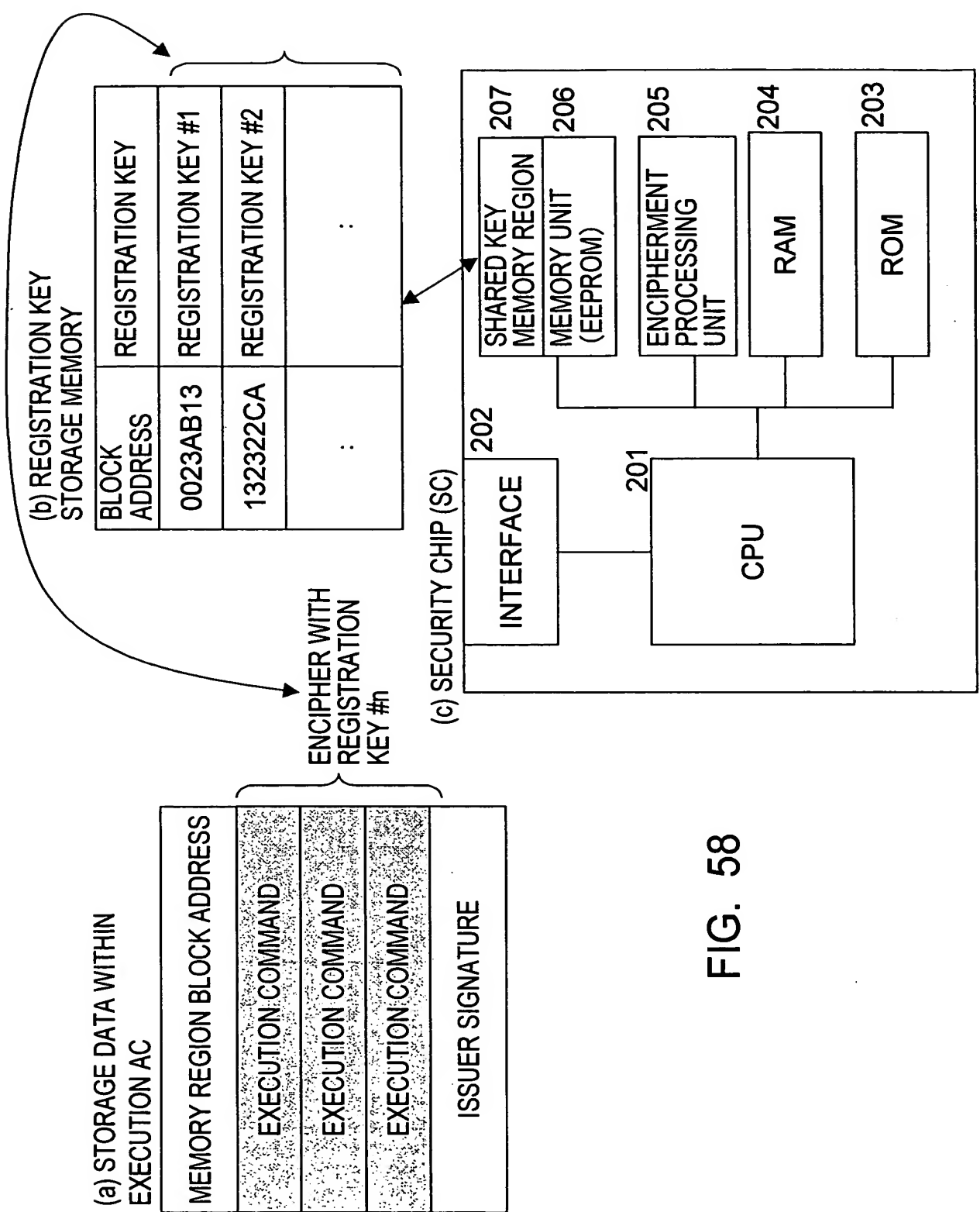


FIG. 58

59/89

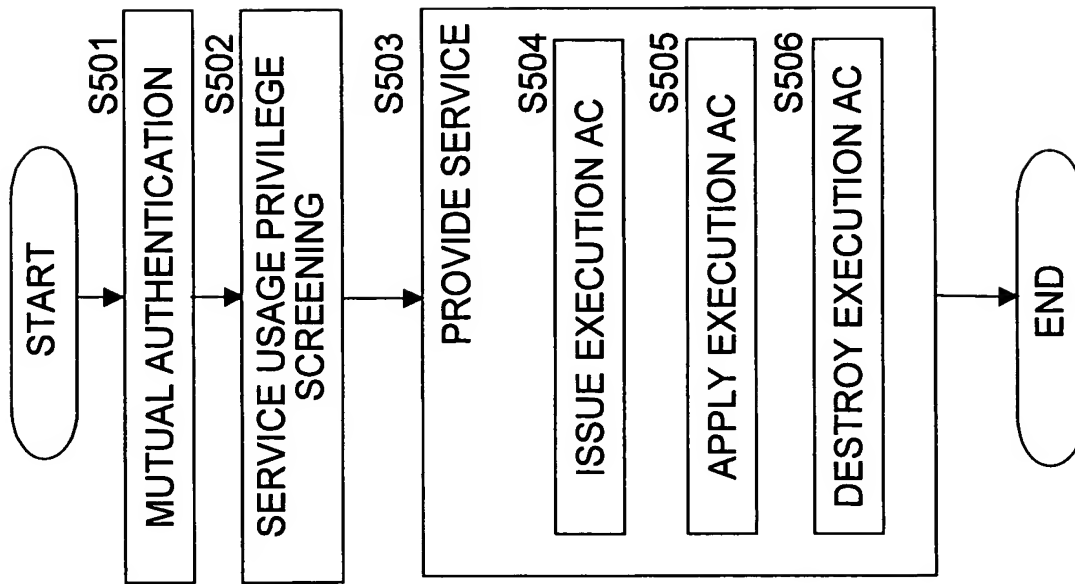


FIG. 59

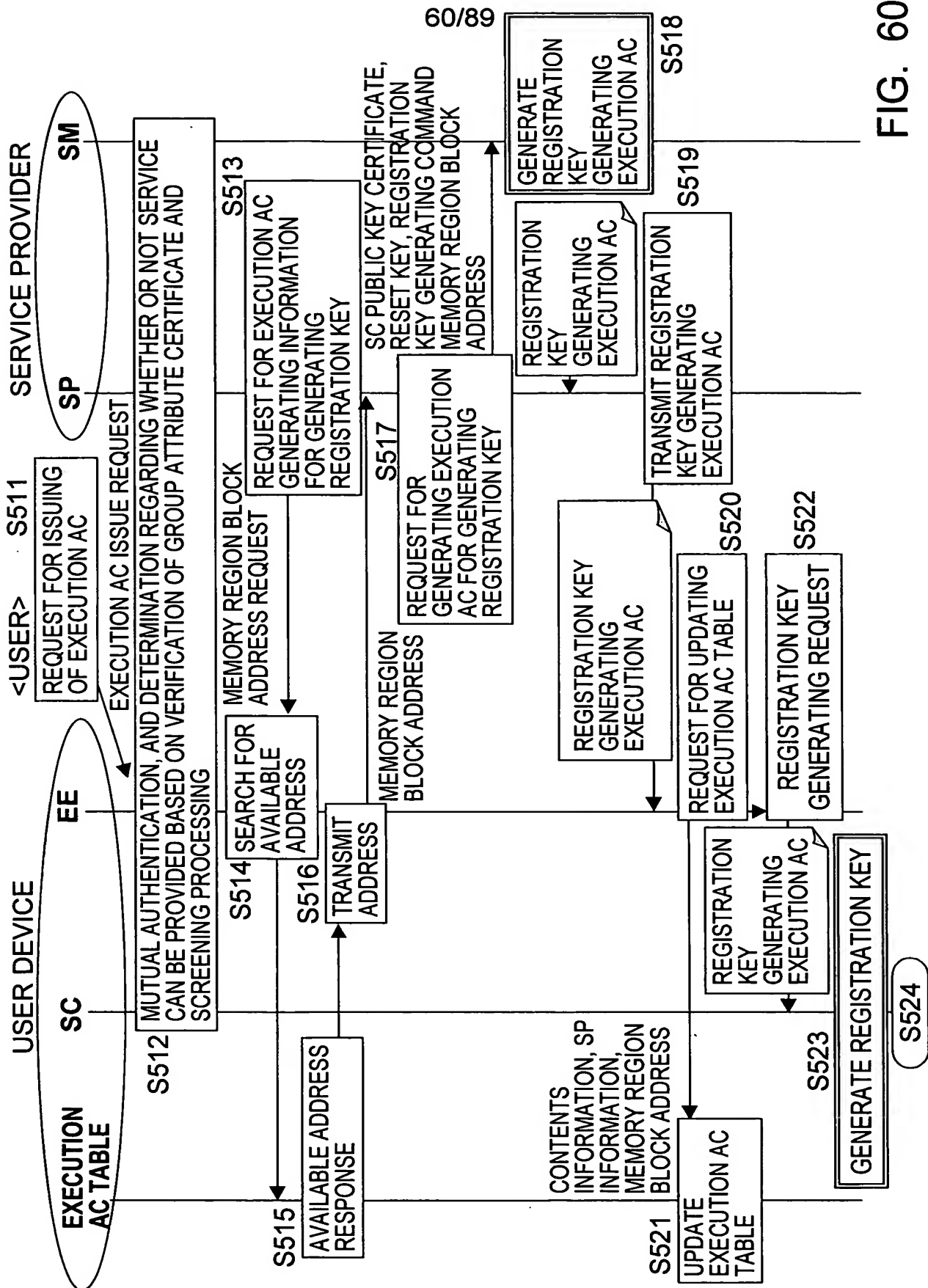


FIG. 60

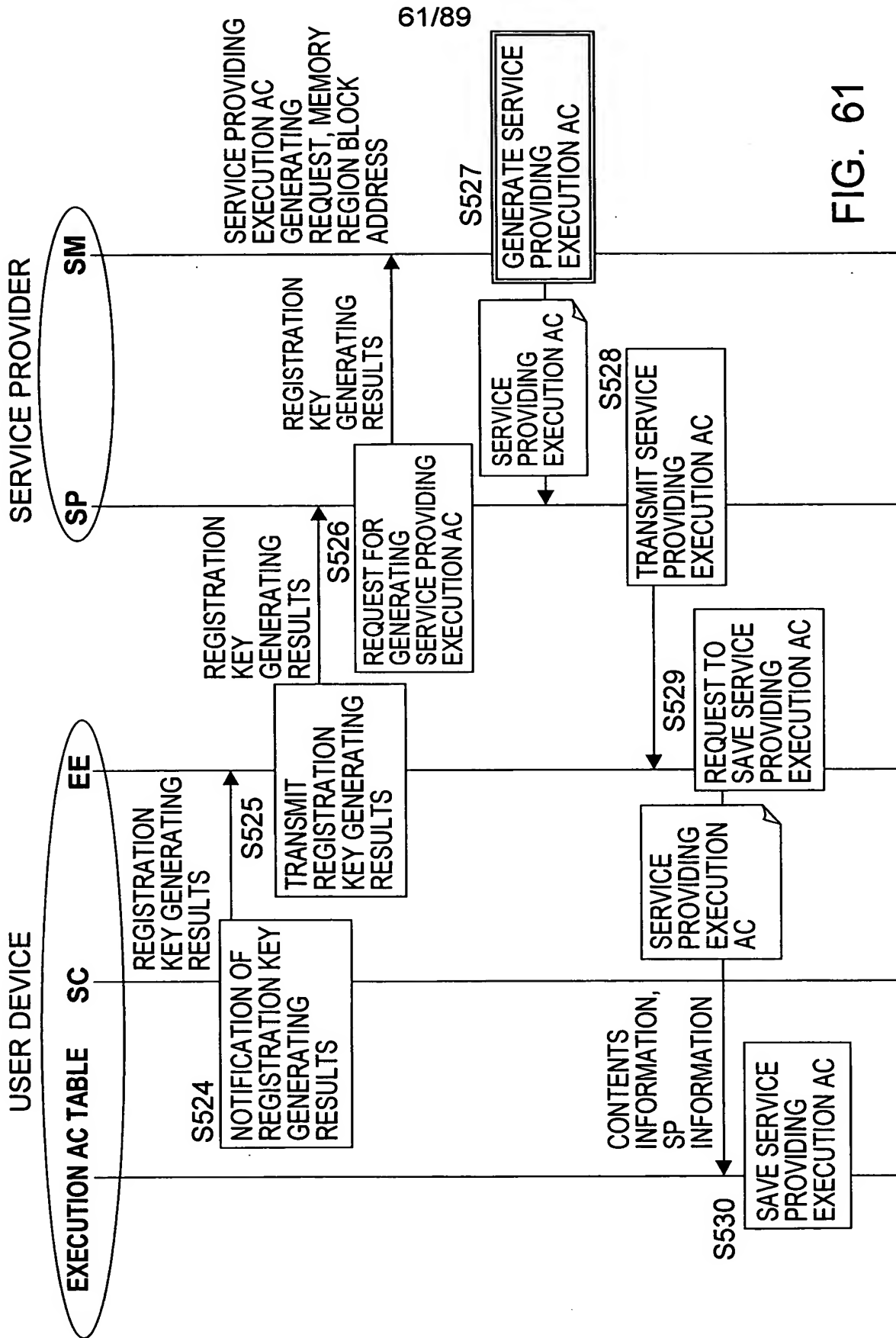
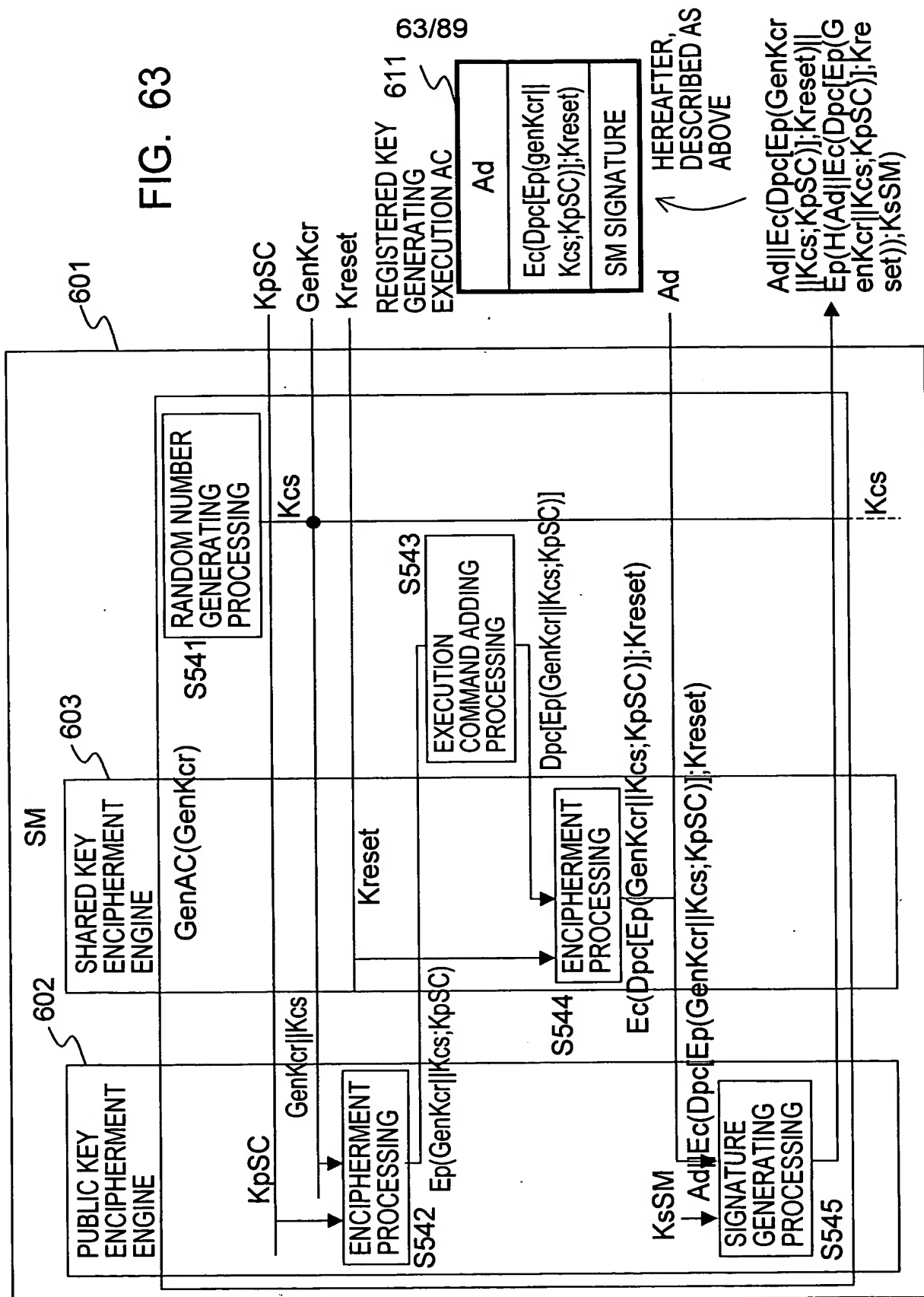


FIG. 61

SP INFORMATION	ENCIPHERED DATA (e.g., CONTENTS) INFORMATION	ENCIPHERED DATA (CONTENTS) DECIPHERING PROCESSING APPLICATION EXECUTION AC
SP_1	ENCIPHERED DATA 1	EXECUTION AC 0001
	ENCIPHERED DATA 2	EXECUTION AC 0002
SP_2	ENCIPHERED DATA 11	...
	ENCIPHERED DATA 12	
	ENCIPHERED DATA 13	

FIG. 62

FIG. 63



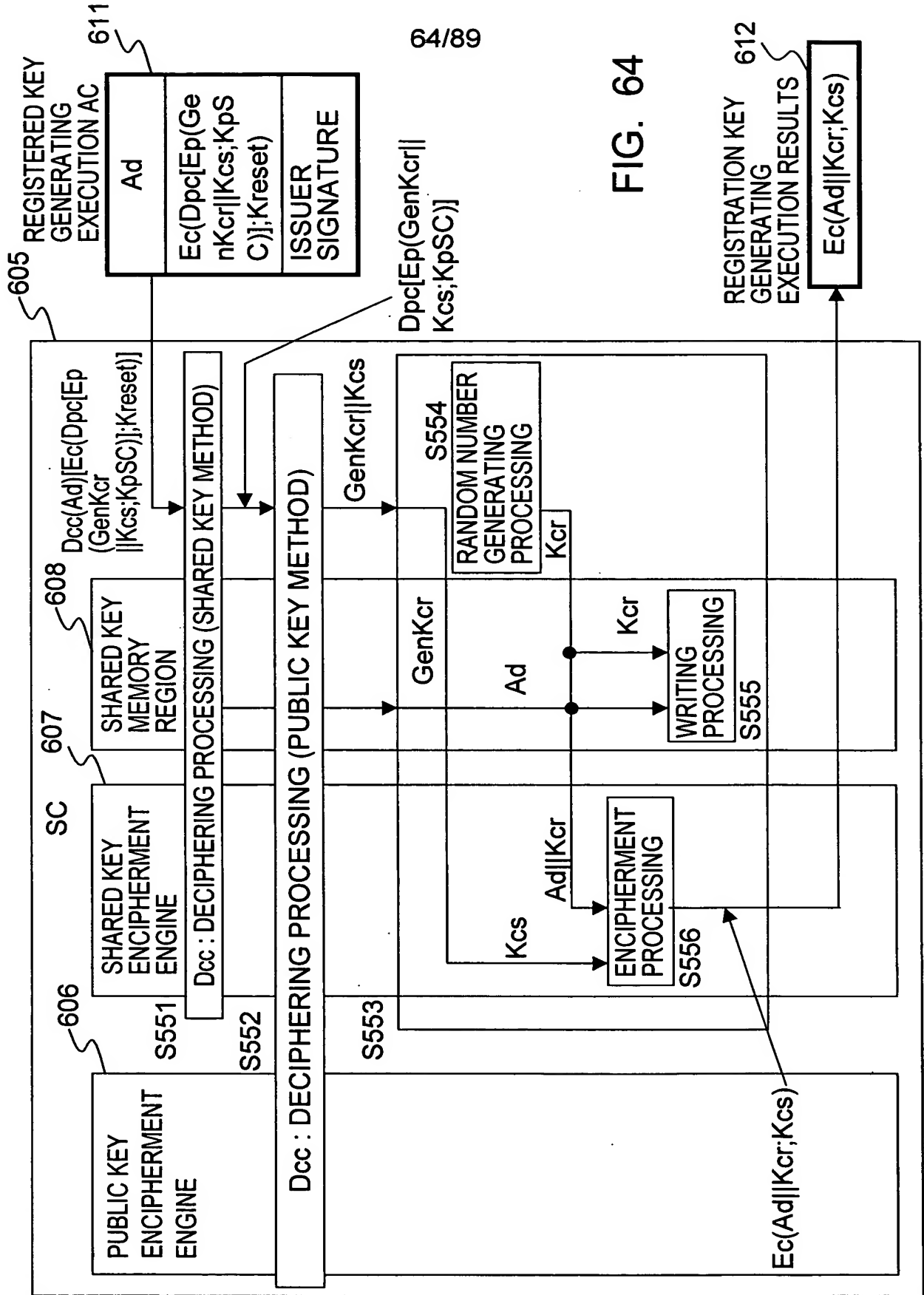
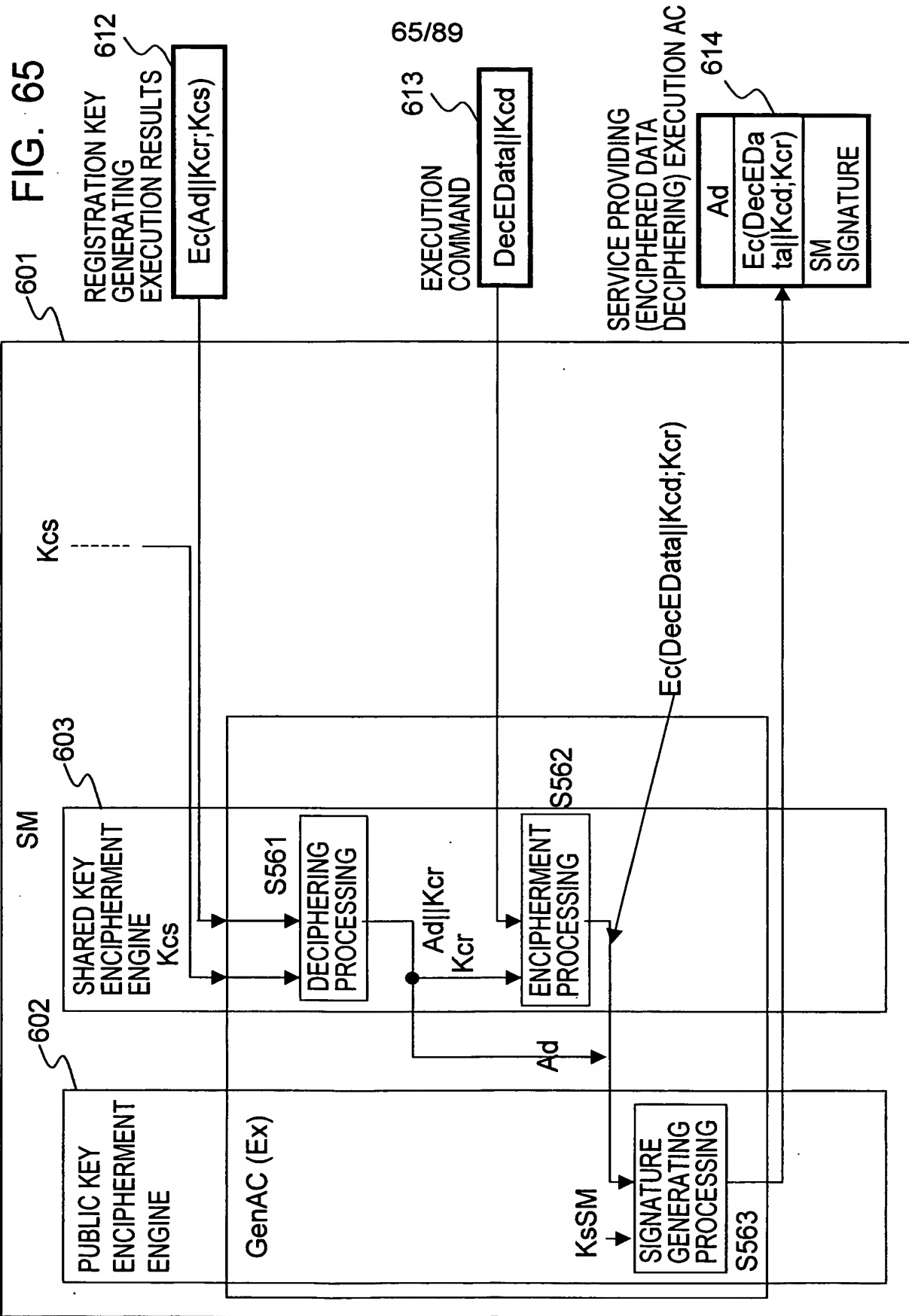


FIG. 64



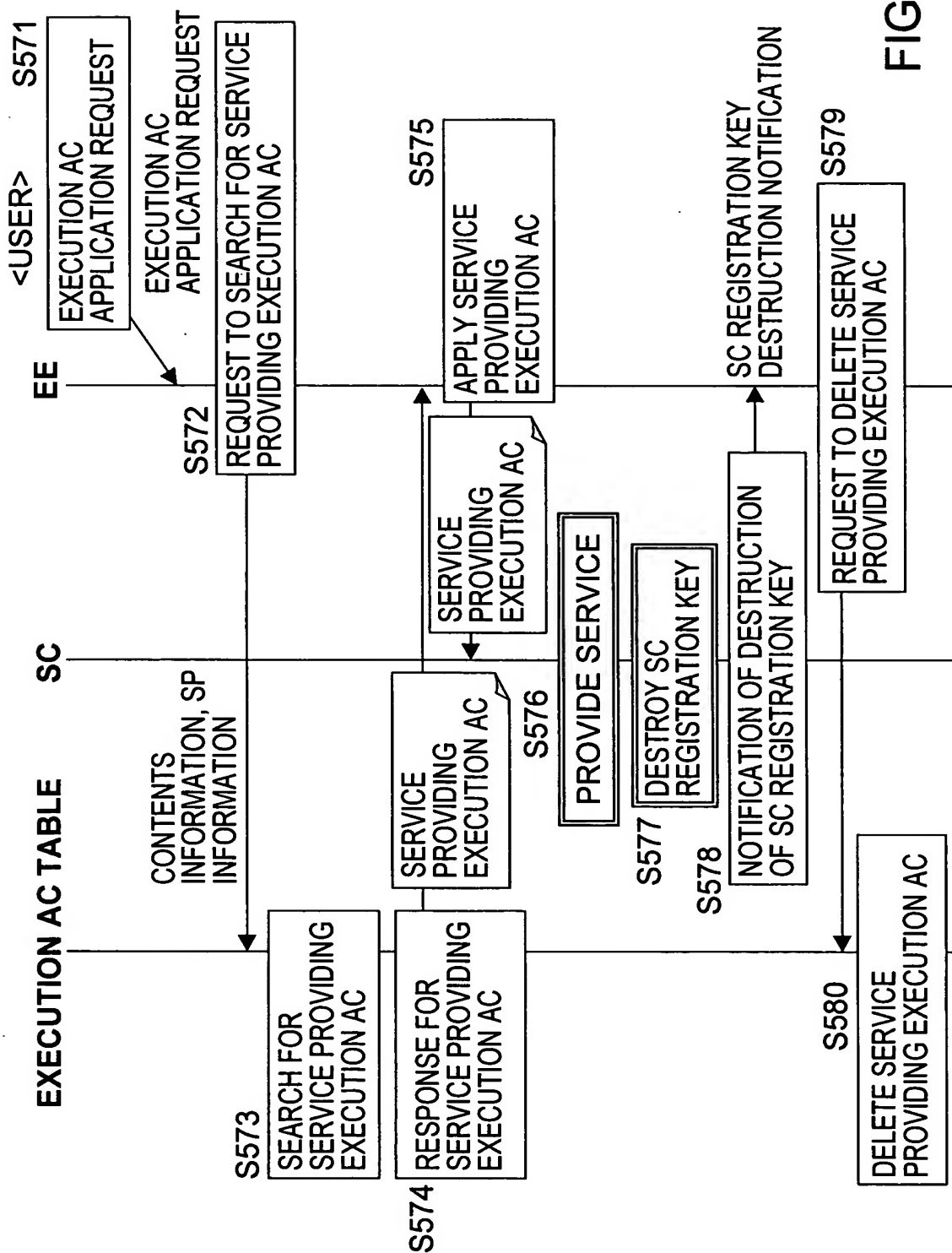


FIG. 66

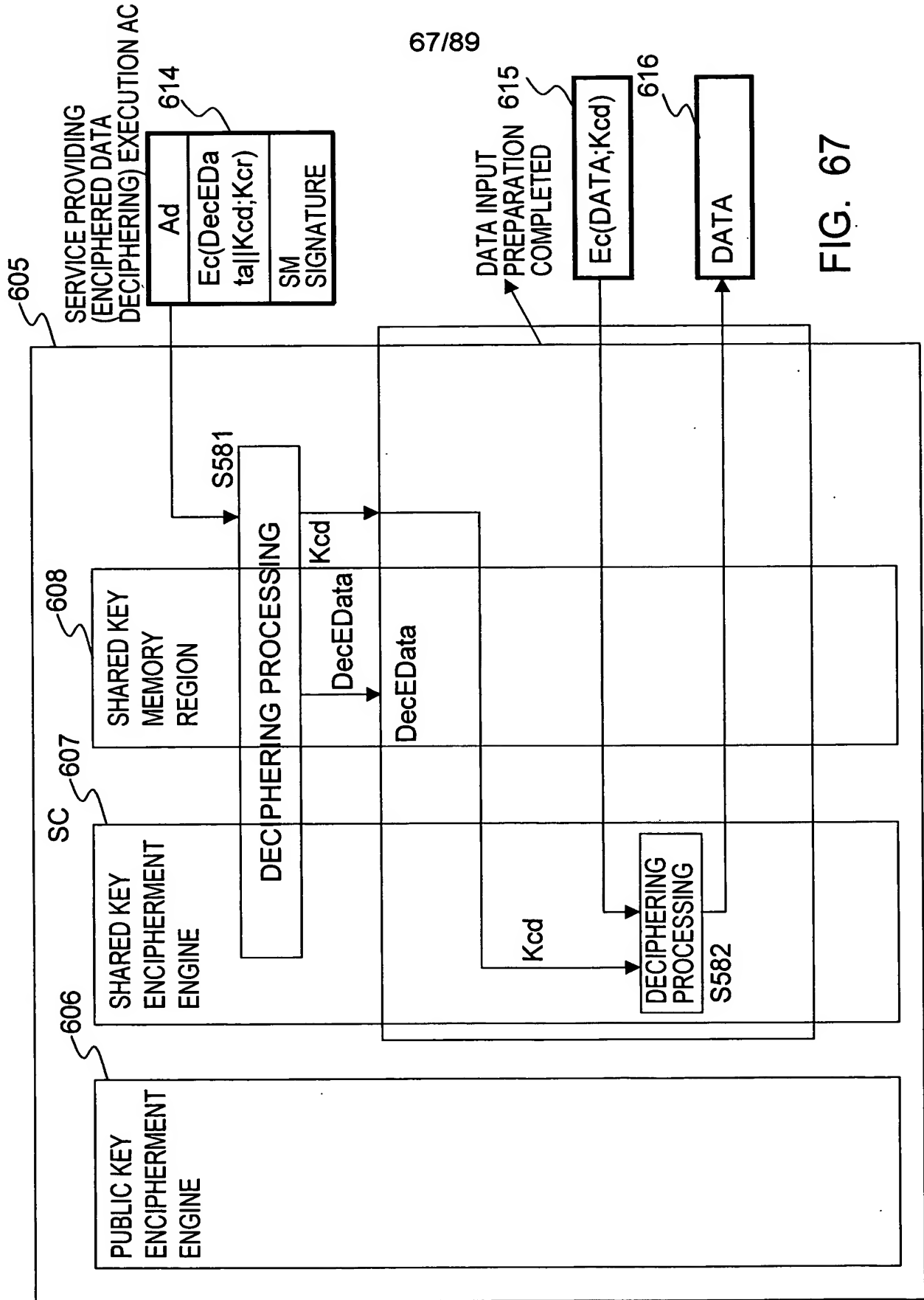


FIG. 67

68/89

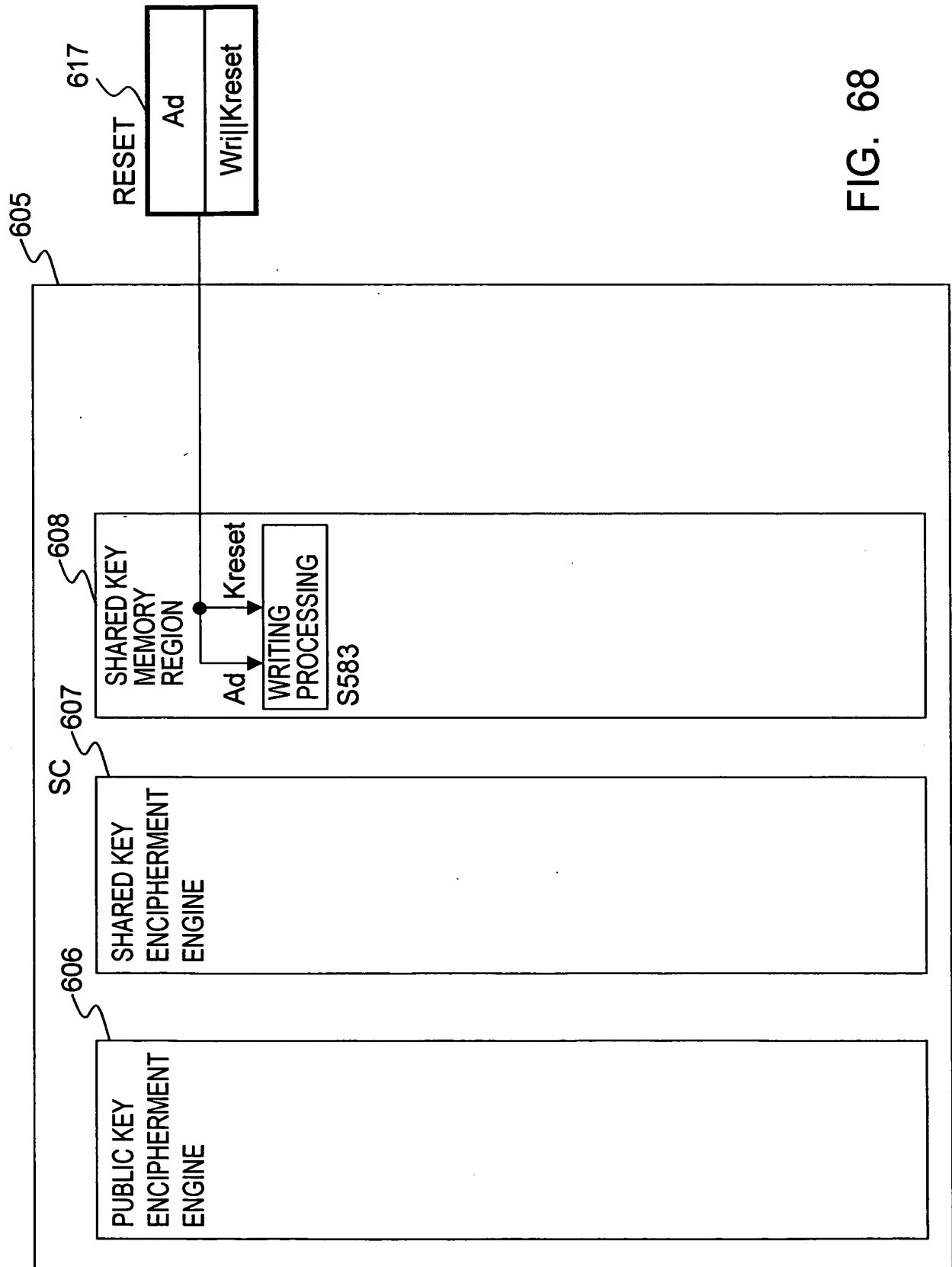


FIG. 68

69/89

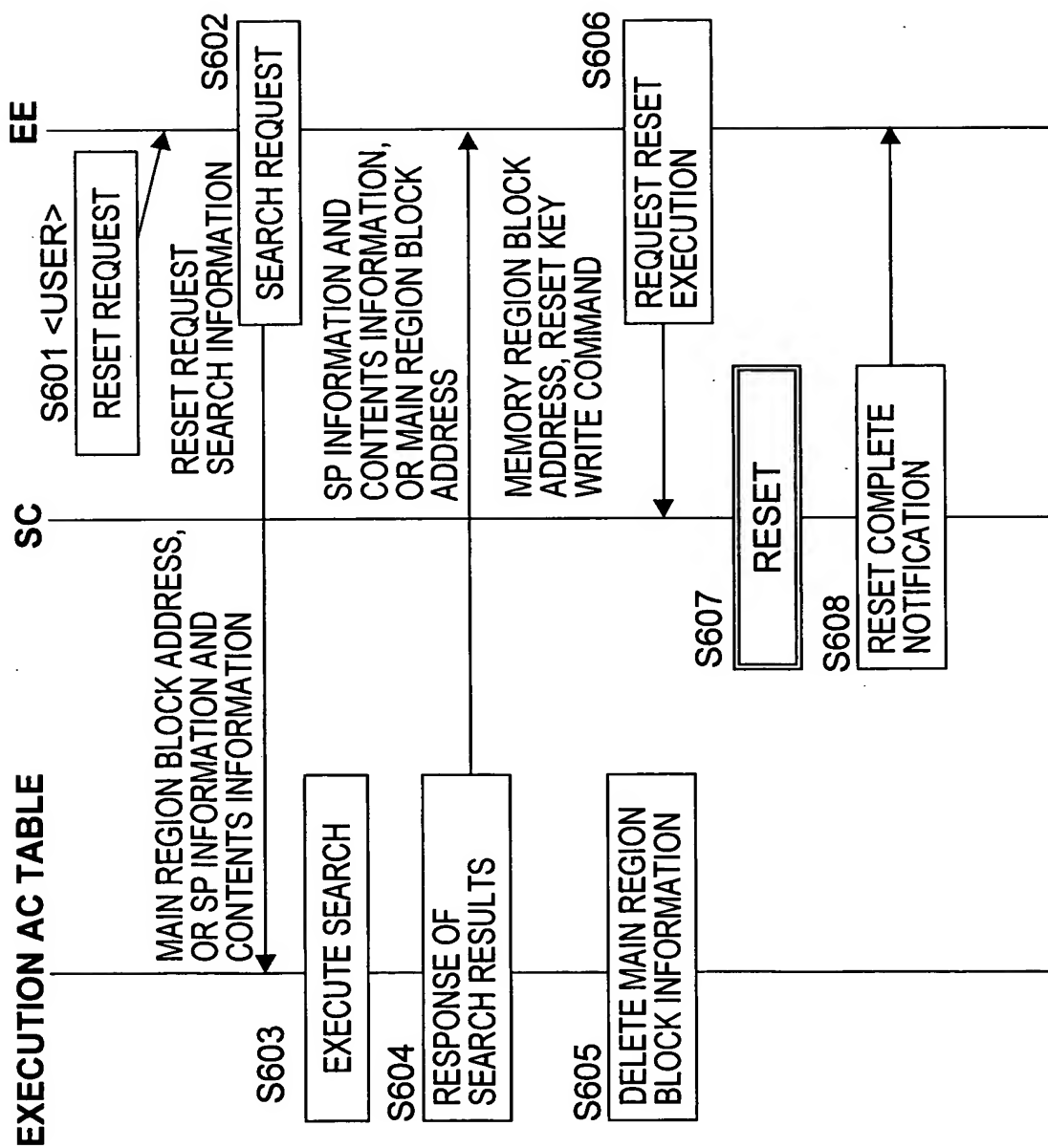


FIG. 69

70/89

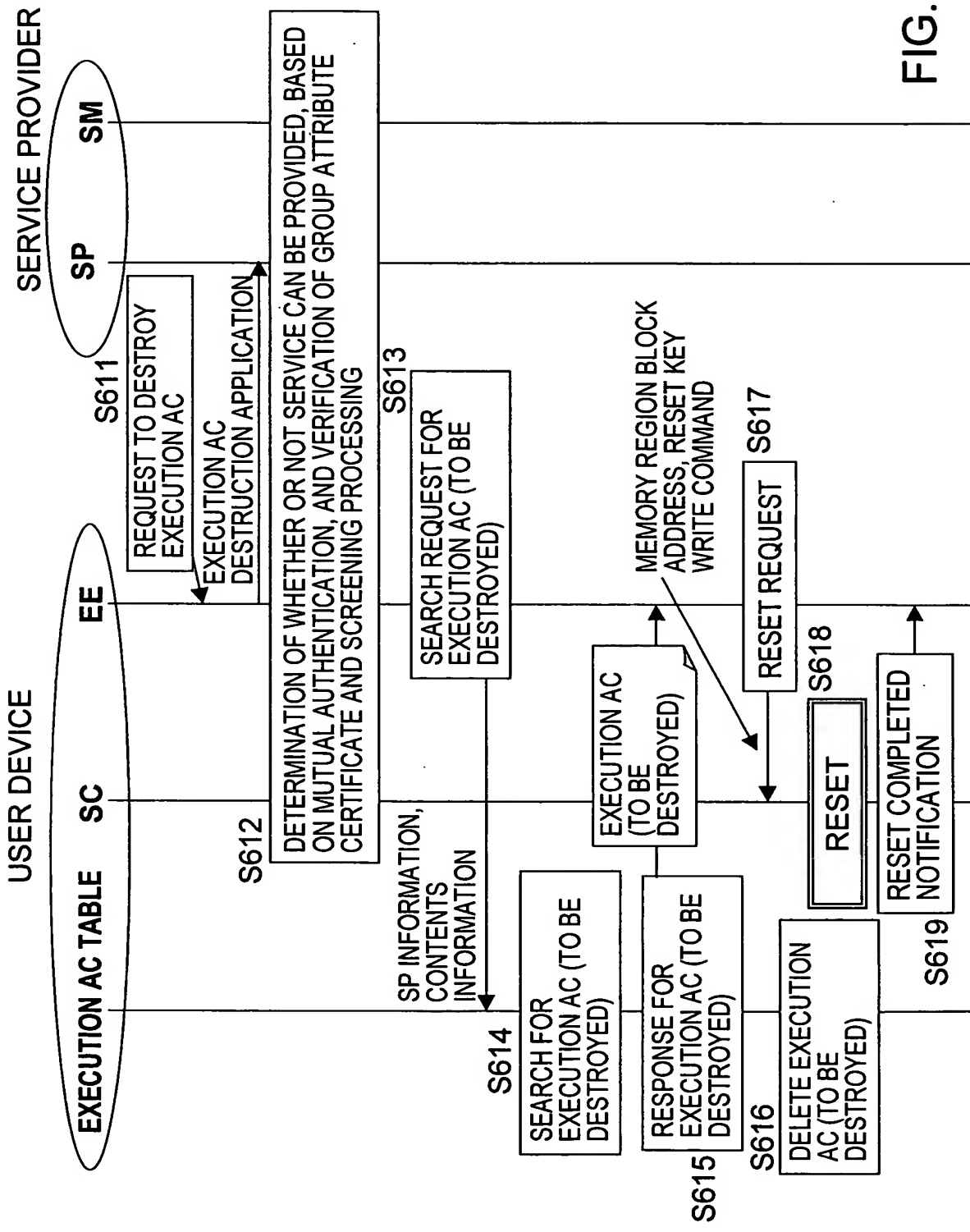
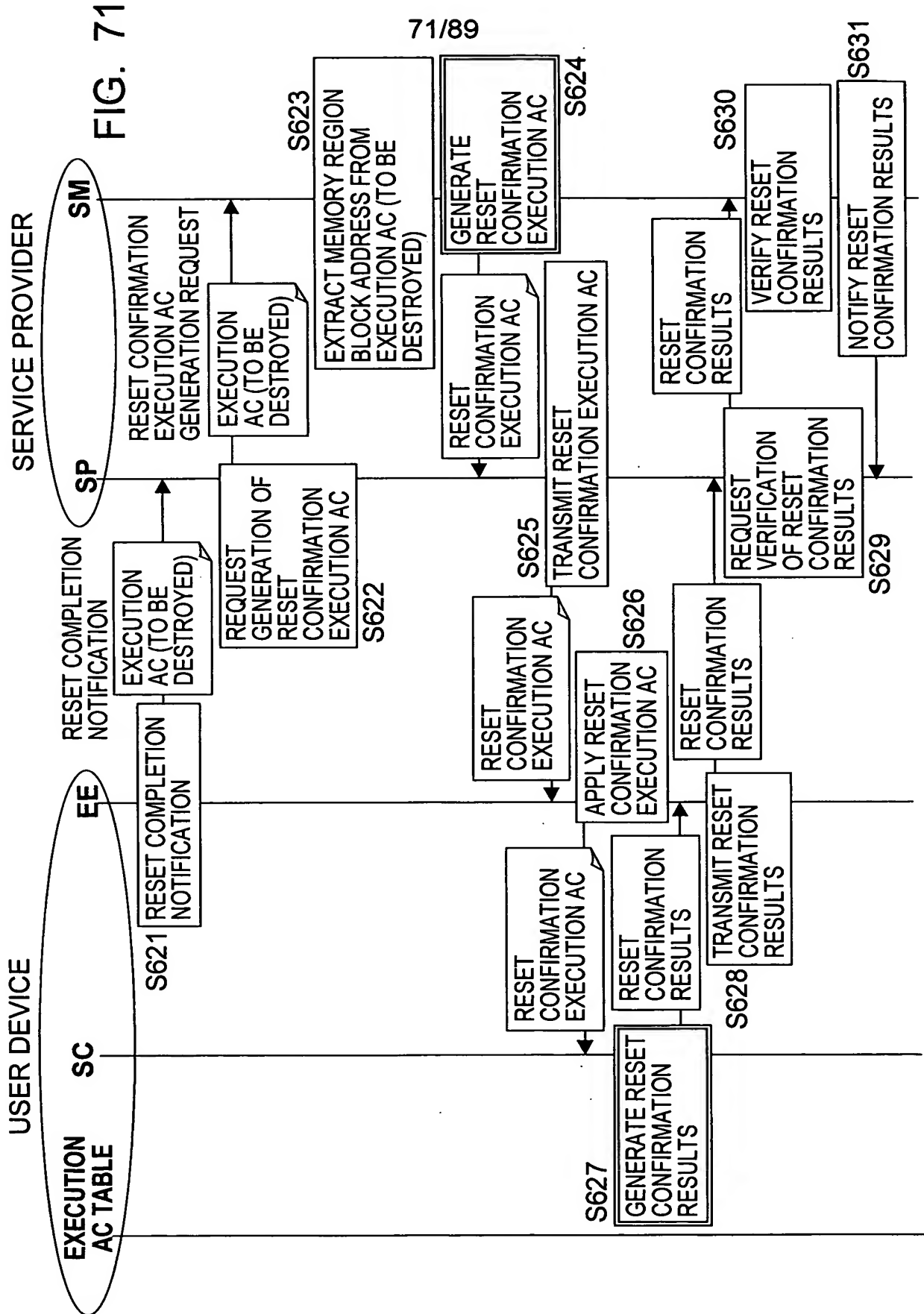
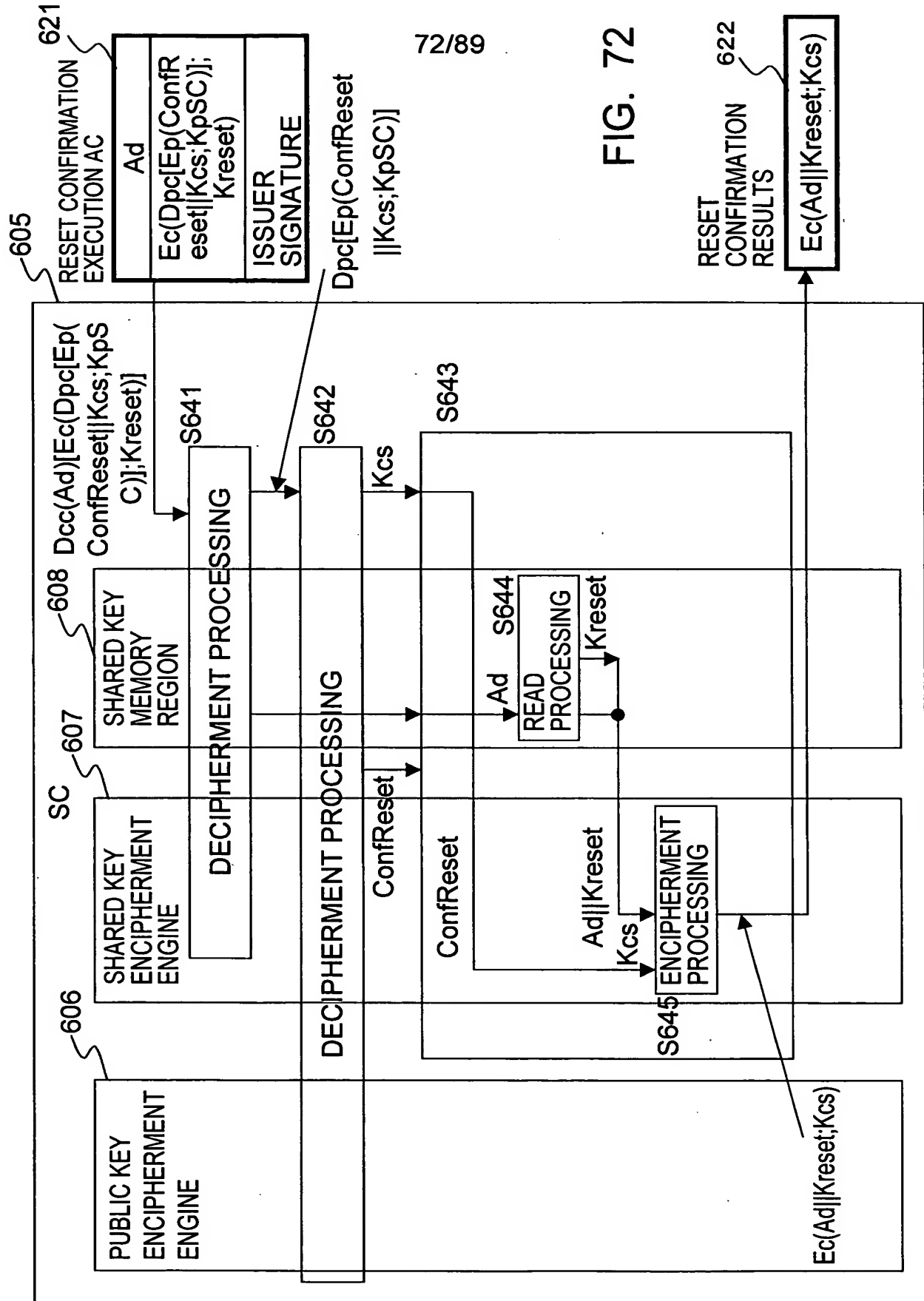


FIG. 70





73/89

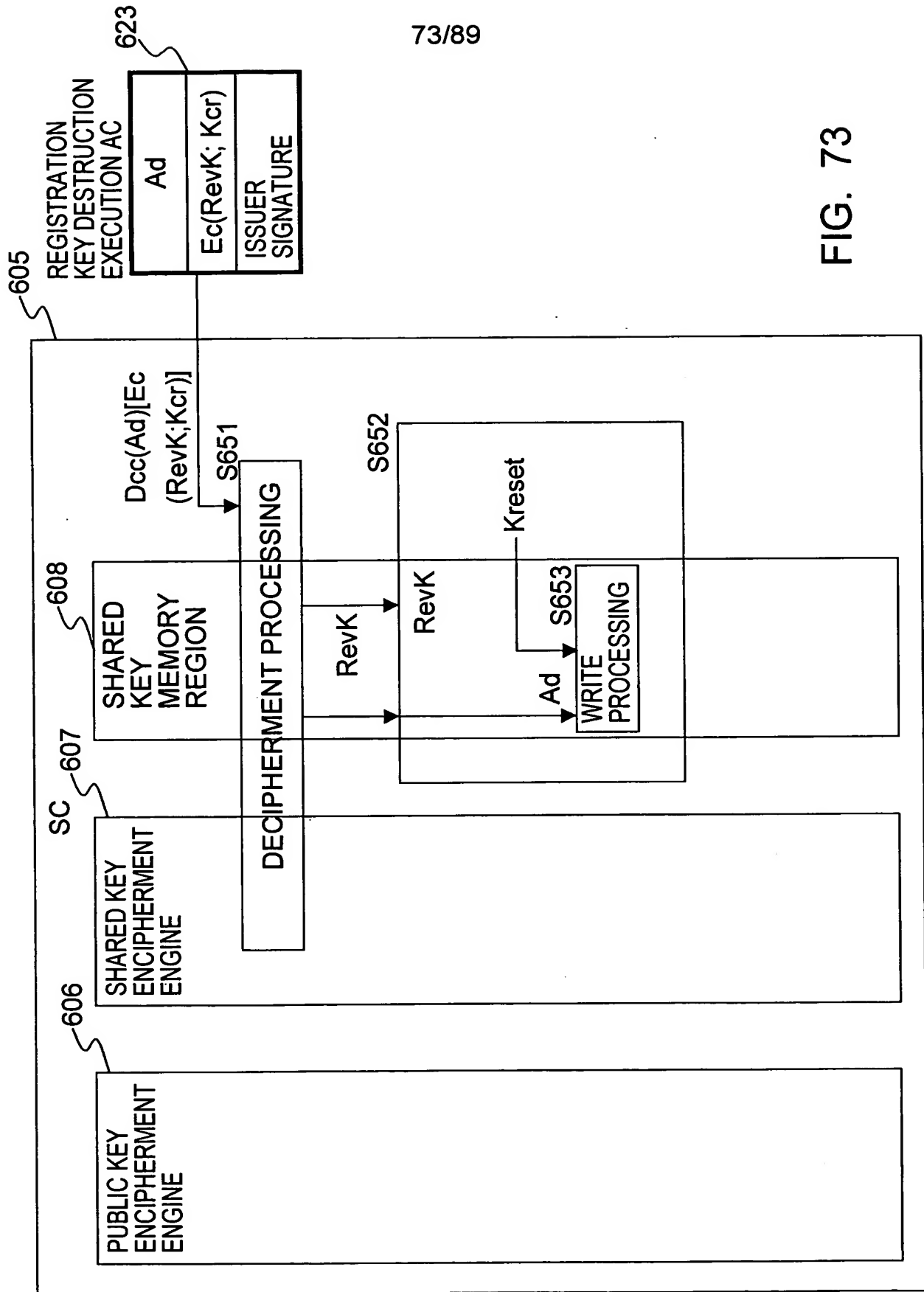


FIG. 73

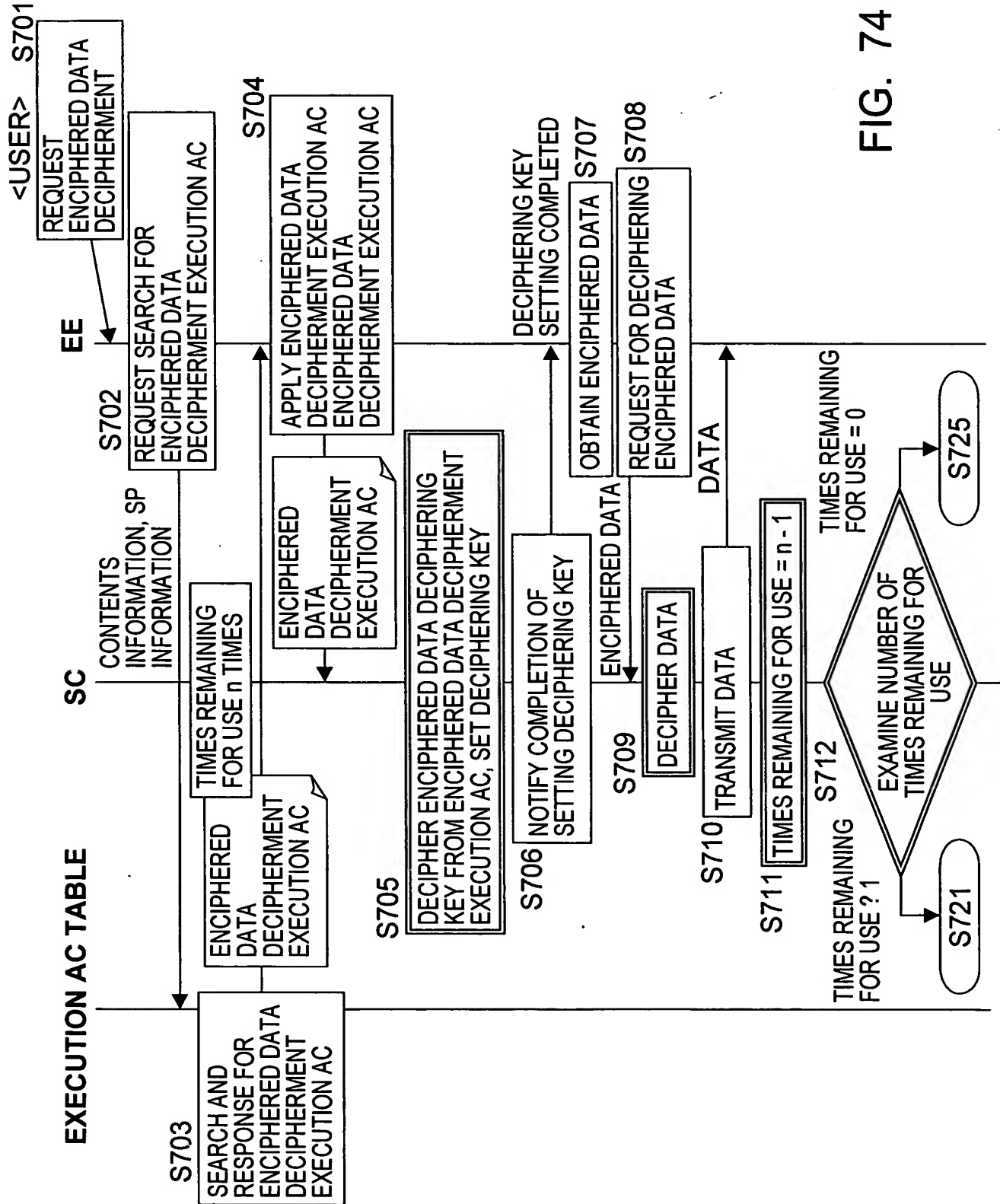


FIG. 74

(A) CASE OF TIMES REMAINING FOR USE BEING 1 OR GREATER FOLLOWING DATA DECIPHERMENT ($n \geq 2$)

(B) CASE OF TIMES REMAINING FOR USE BEING 0 FOLLOWING DATA DECIPHERMENT ($n = 1$)

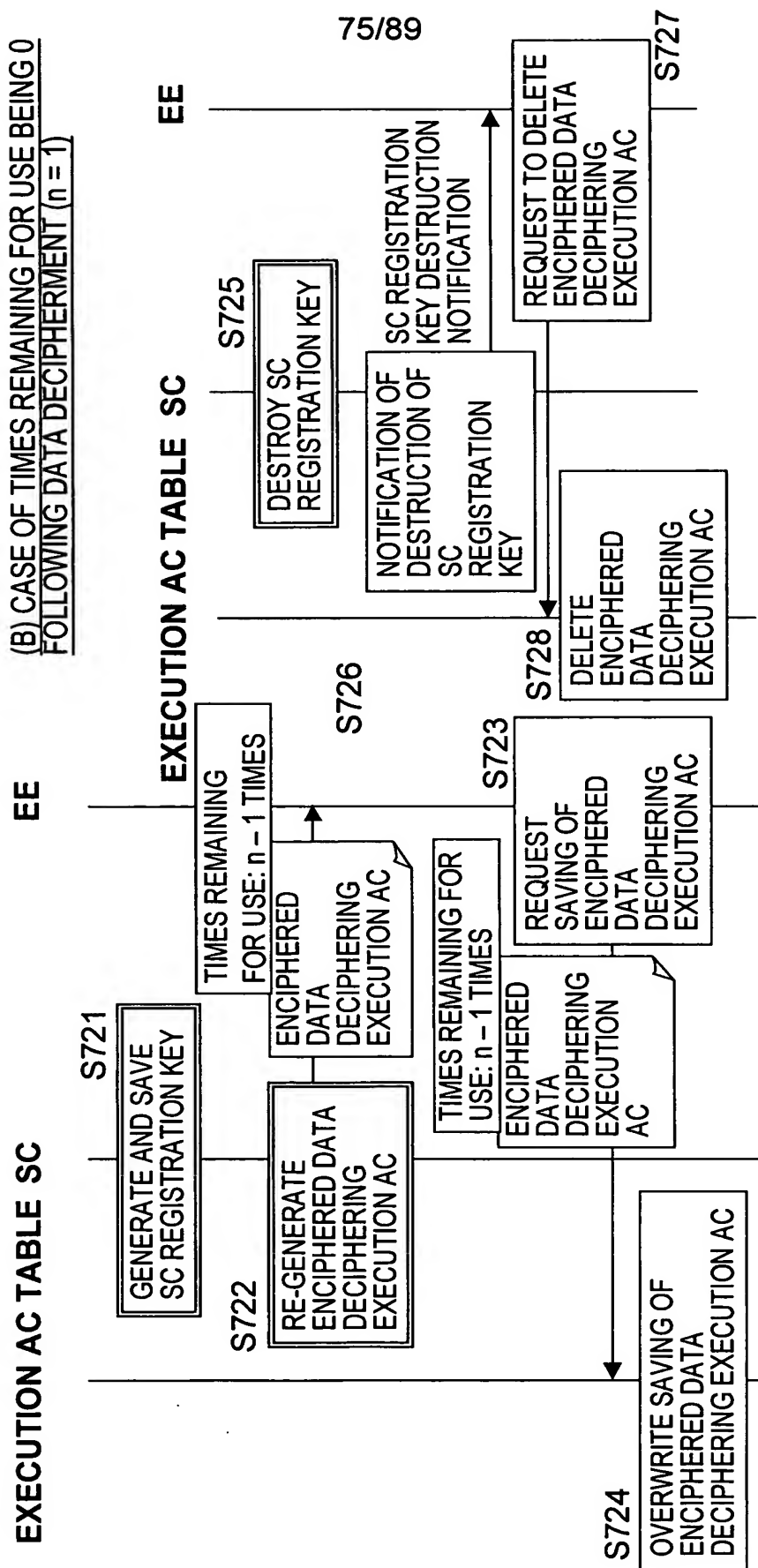
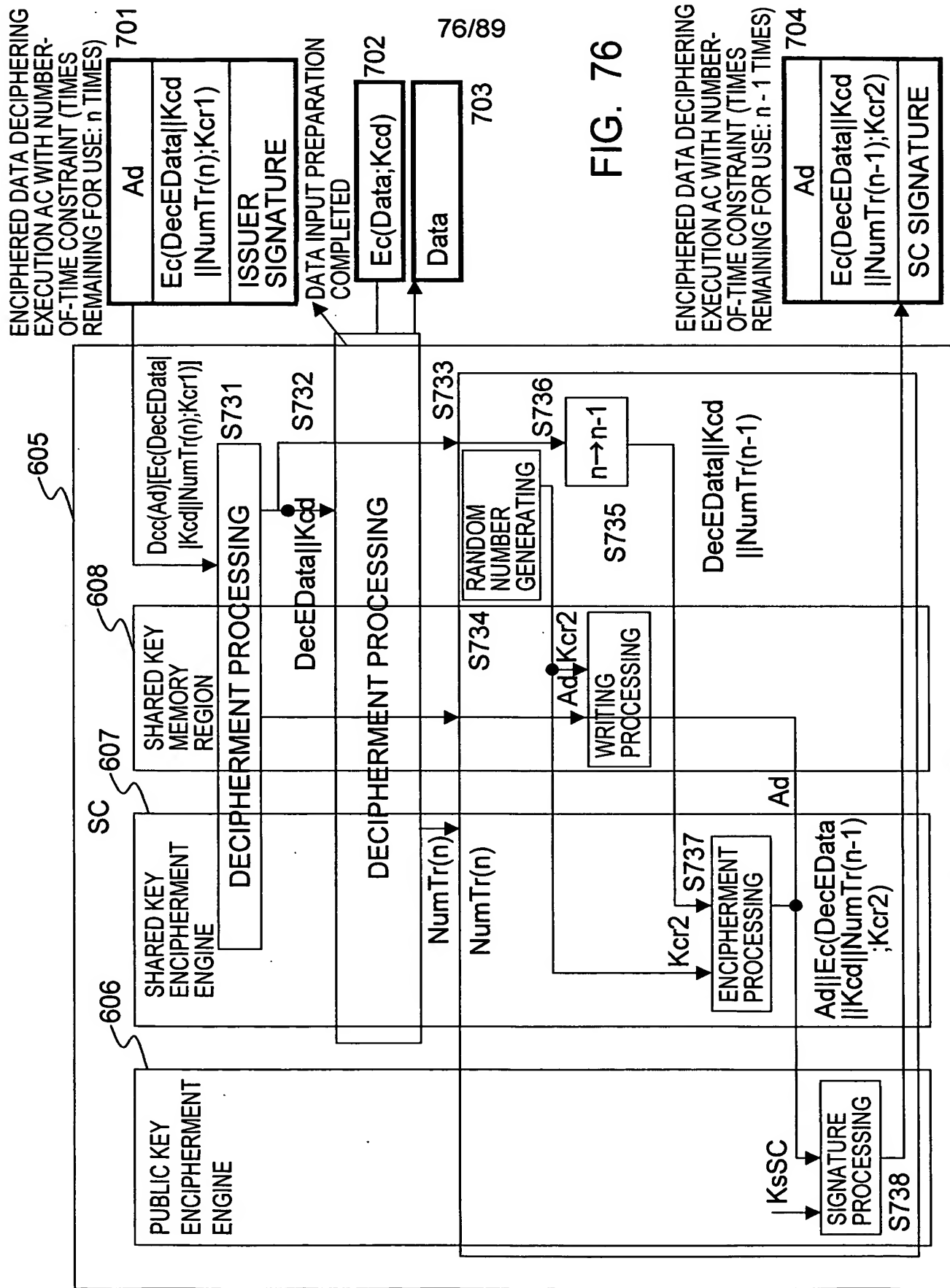


FIG. 75



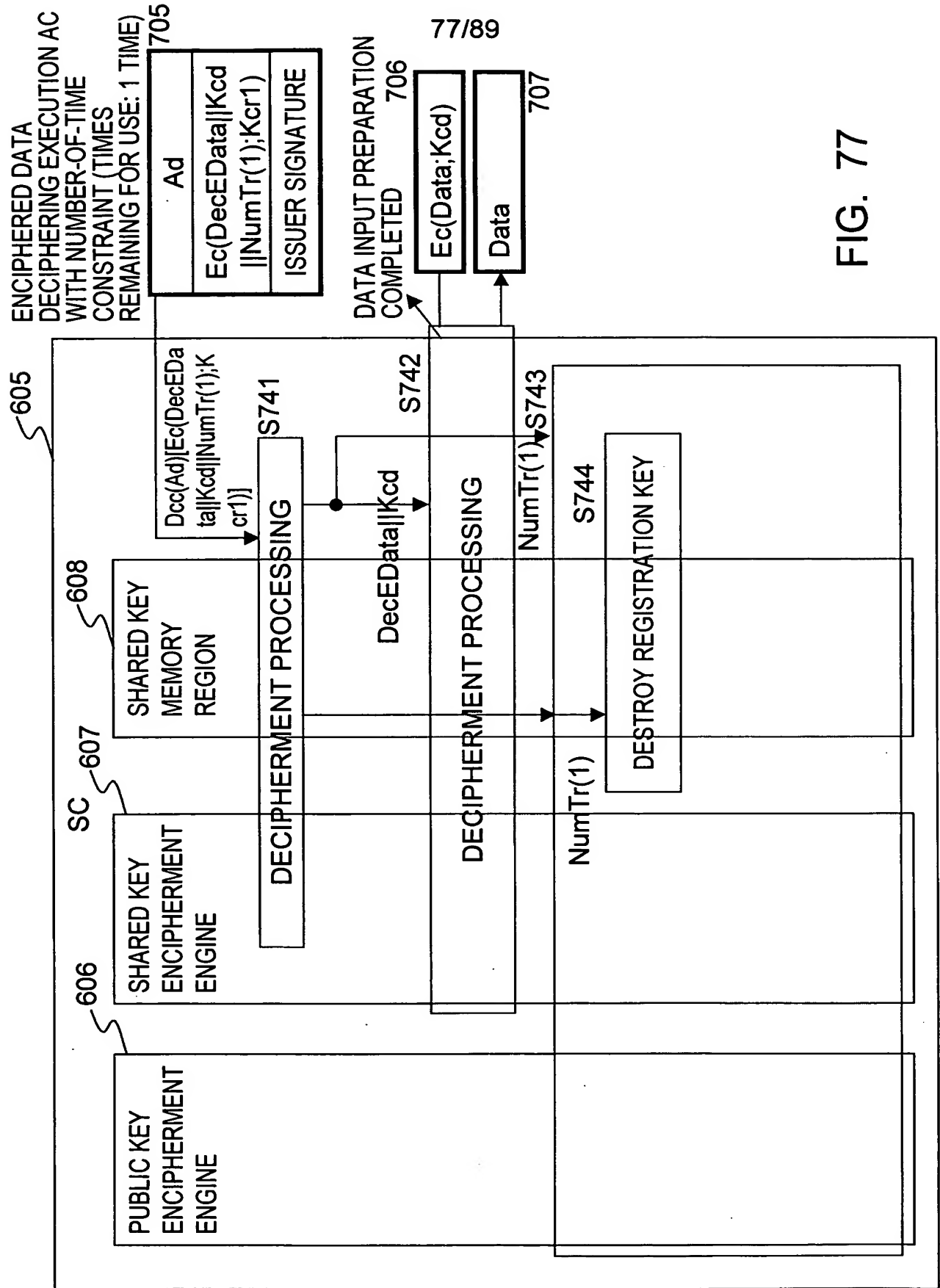
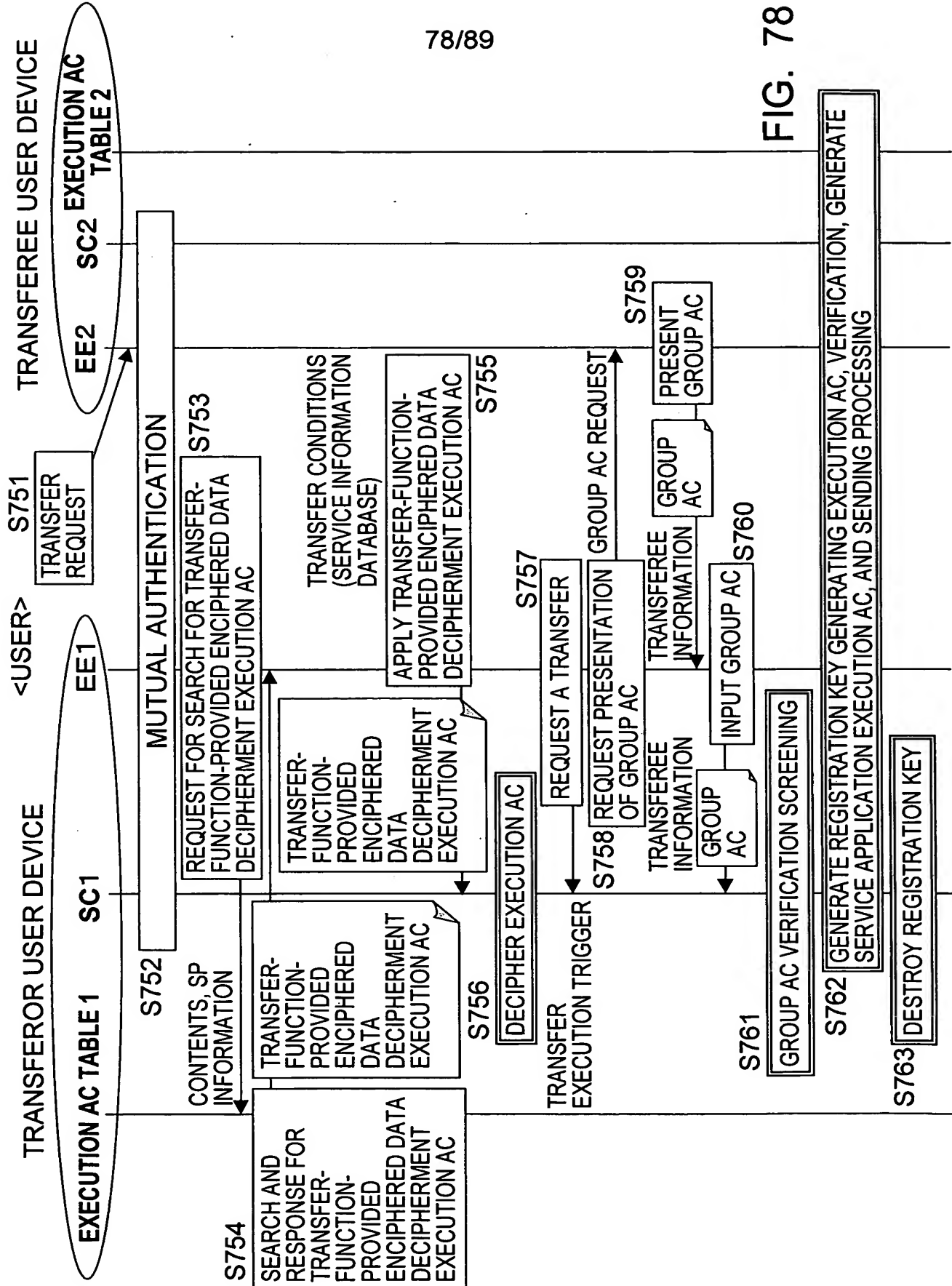
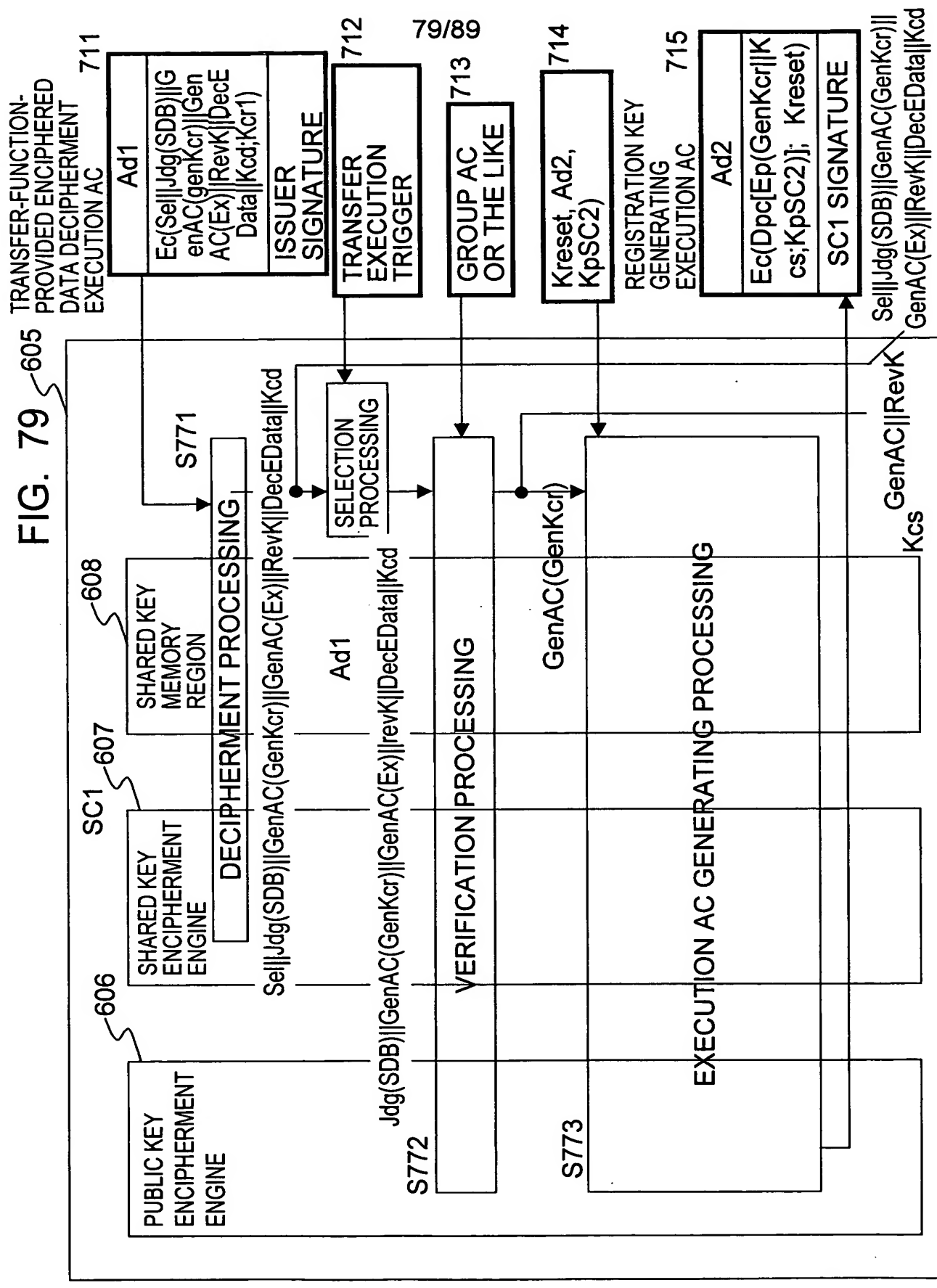


FIG. 77

78/89





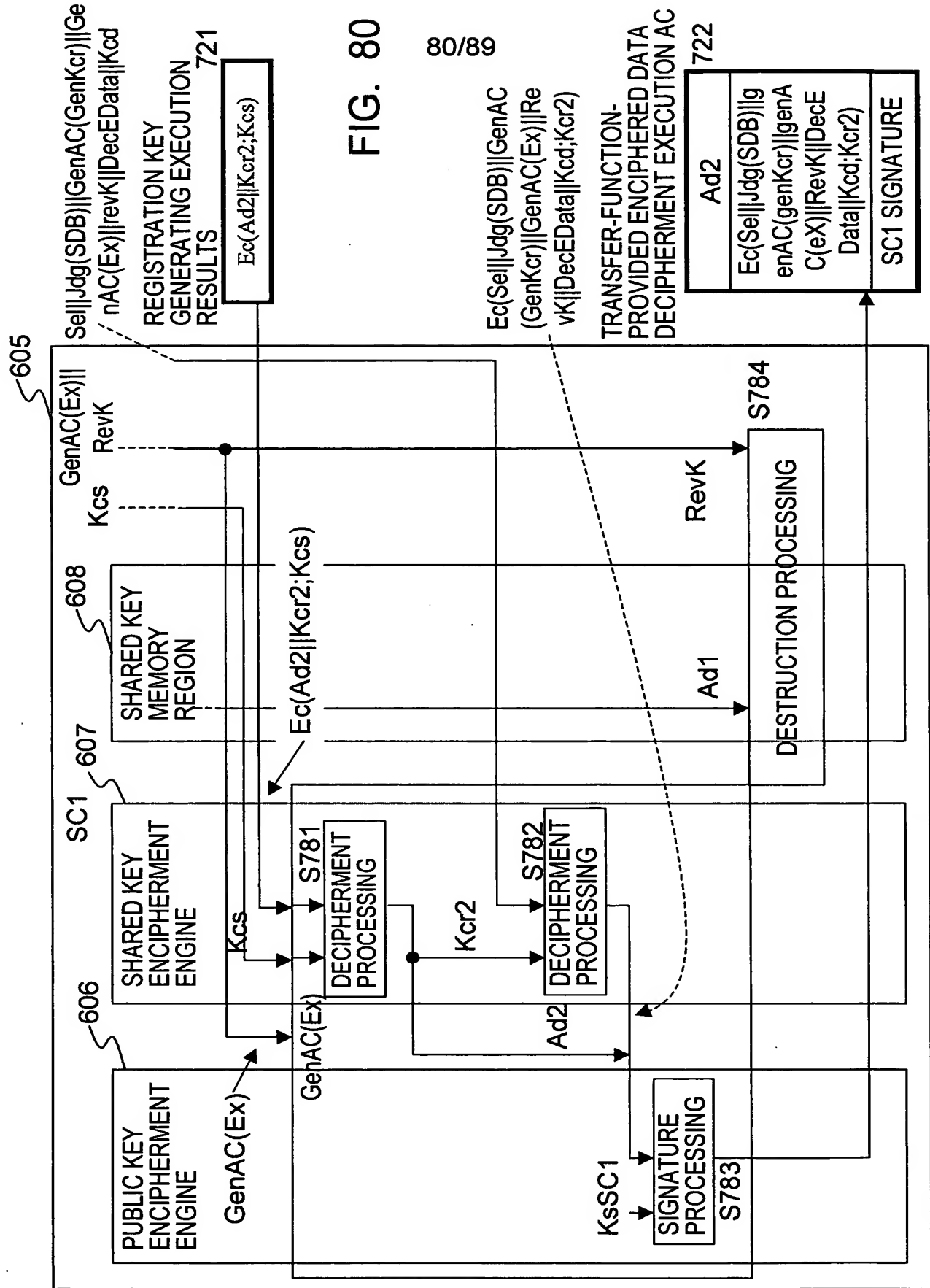


FIG. 80

80/89

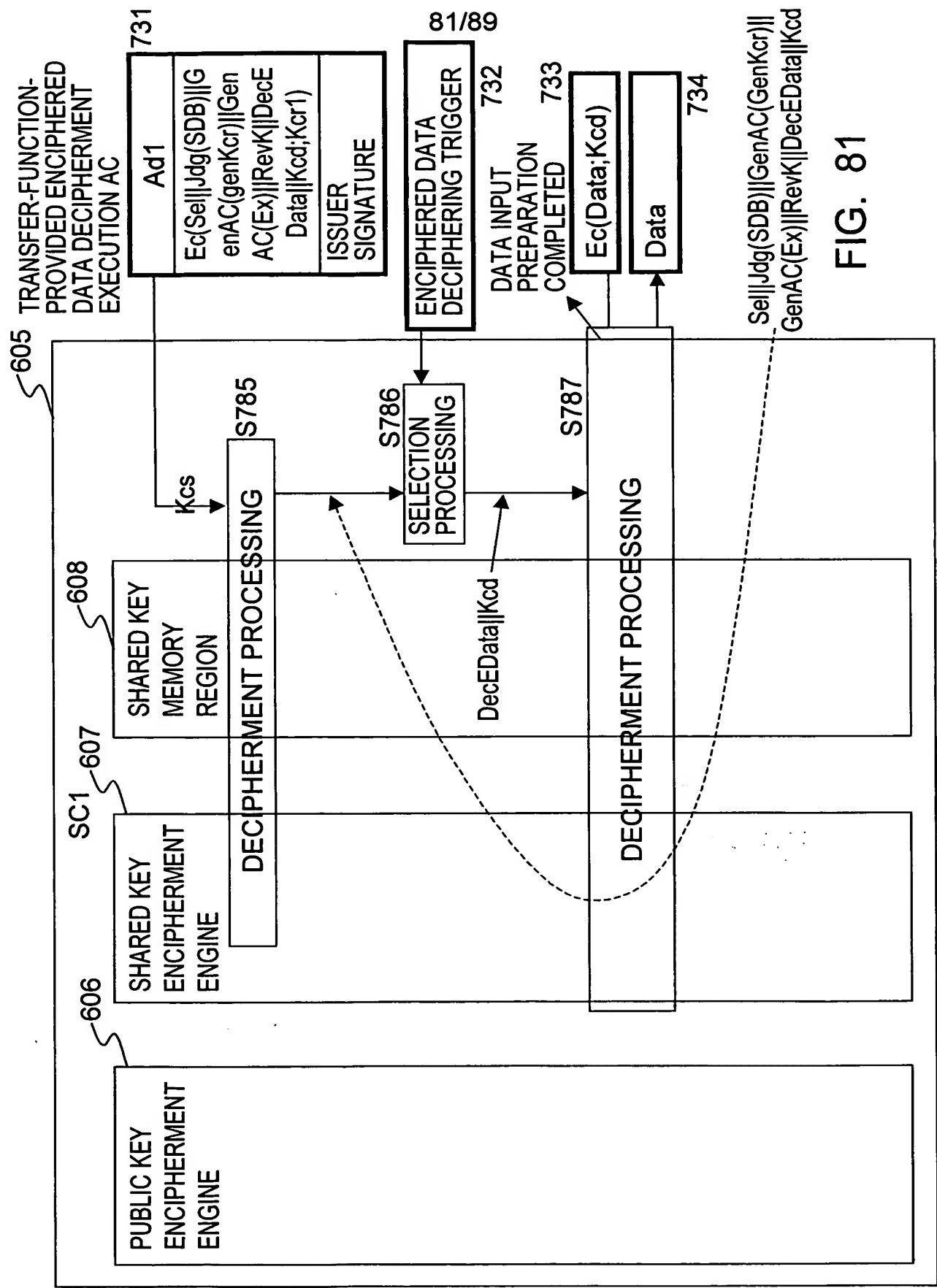
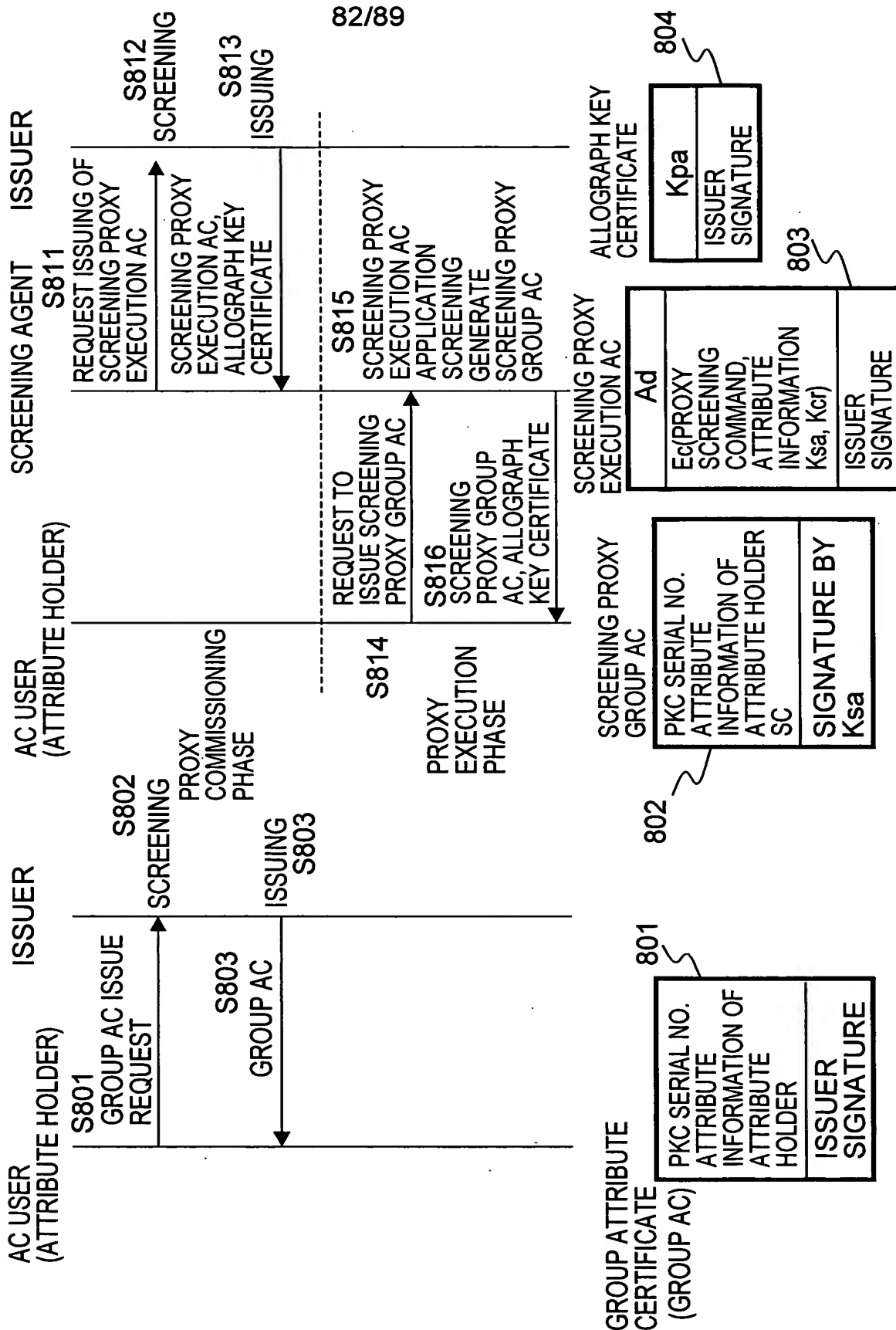


FIG. 82

(a) ISSUING CONFIGURATION FOR NORMAL ATTRIBUTE CERTIFICATE (GROUP AC)

(b) ISSUING CONFIGURATION FOR ATTRIBUTE CERTIFICATE (GROUP AC) APPLYING SCREENING PROXY EXECUTION ATTRIBUTE CERTIFICATE



83/89

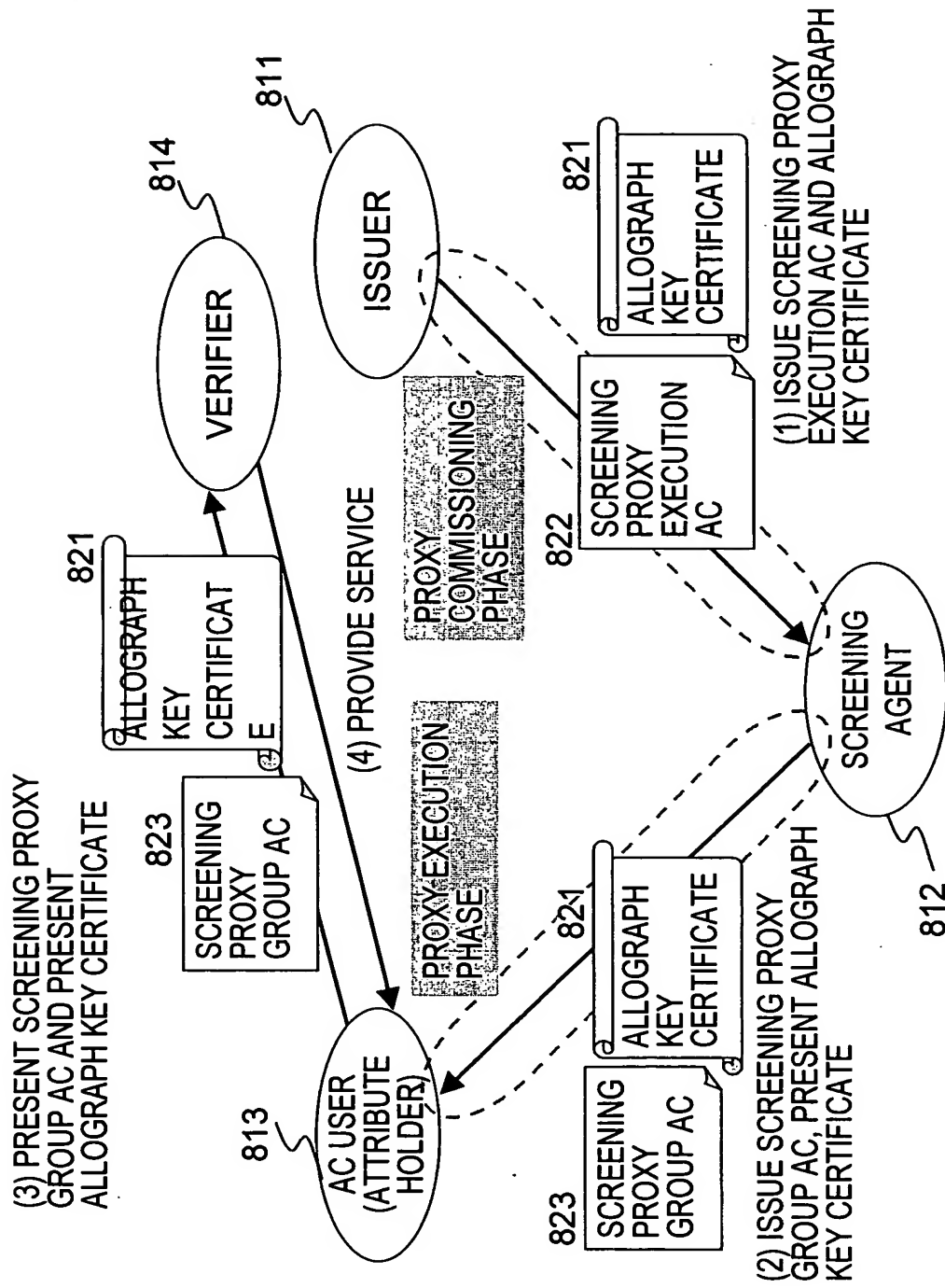


FIG. 83

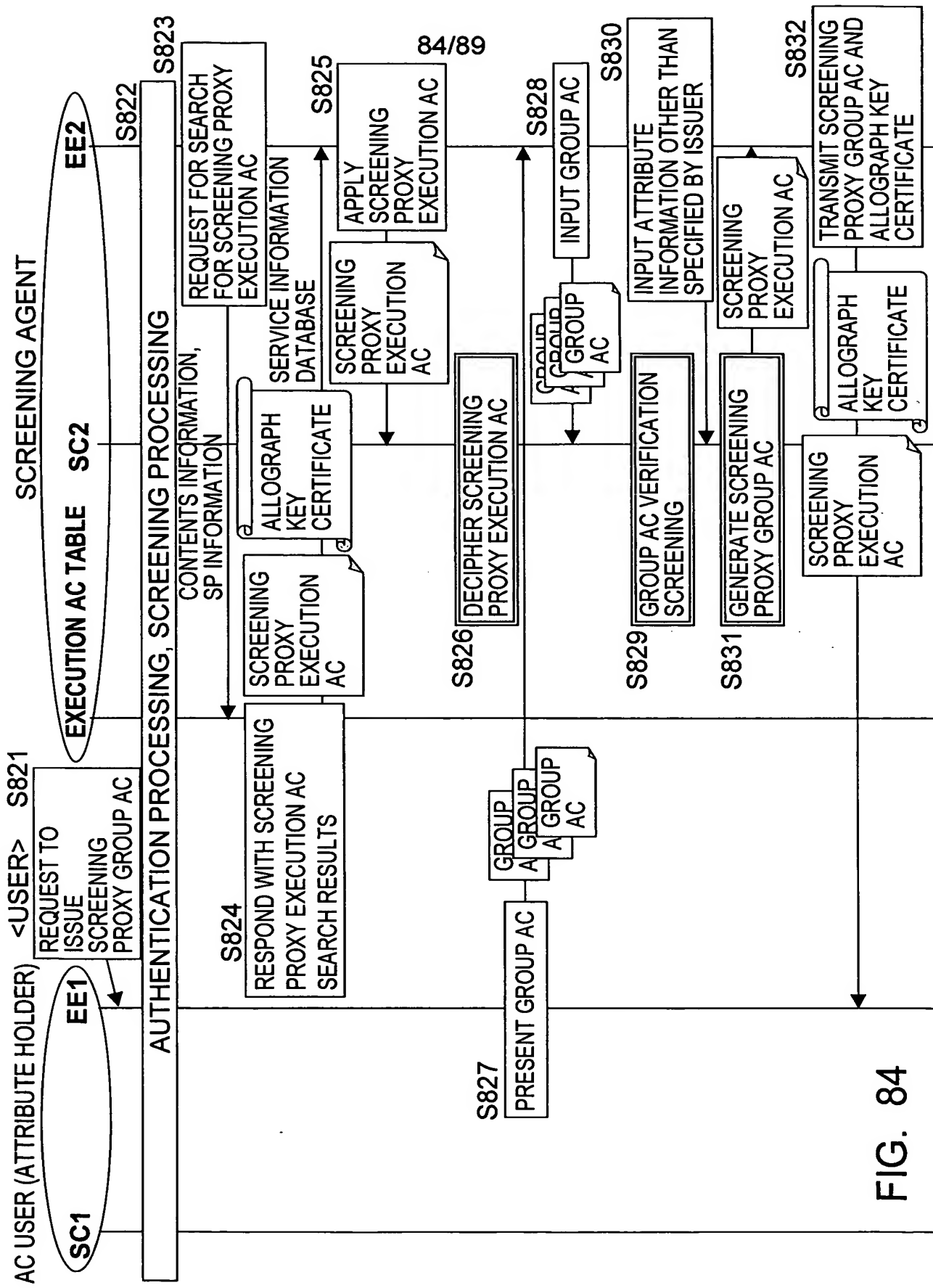


FIG. 84

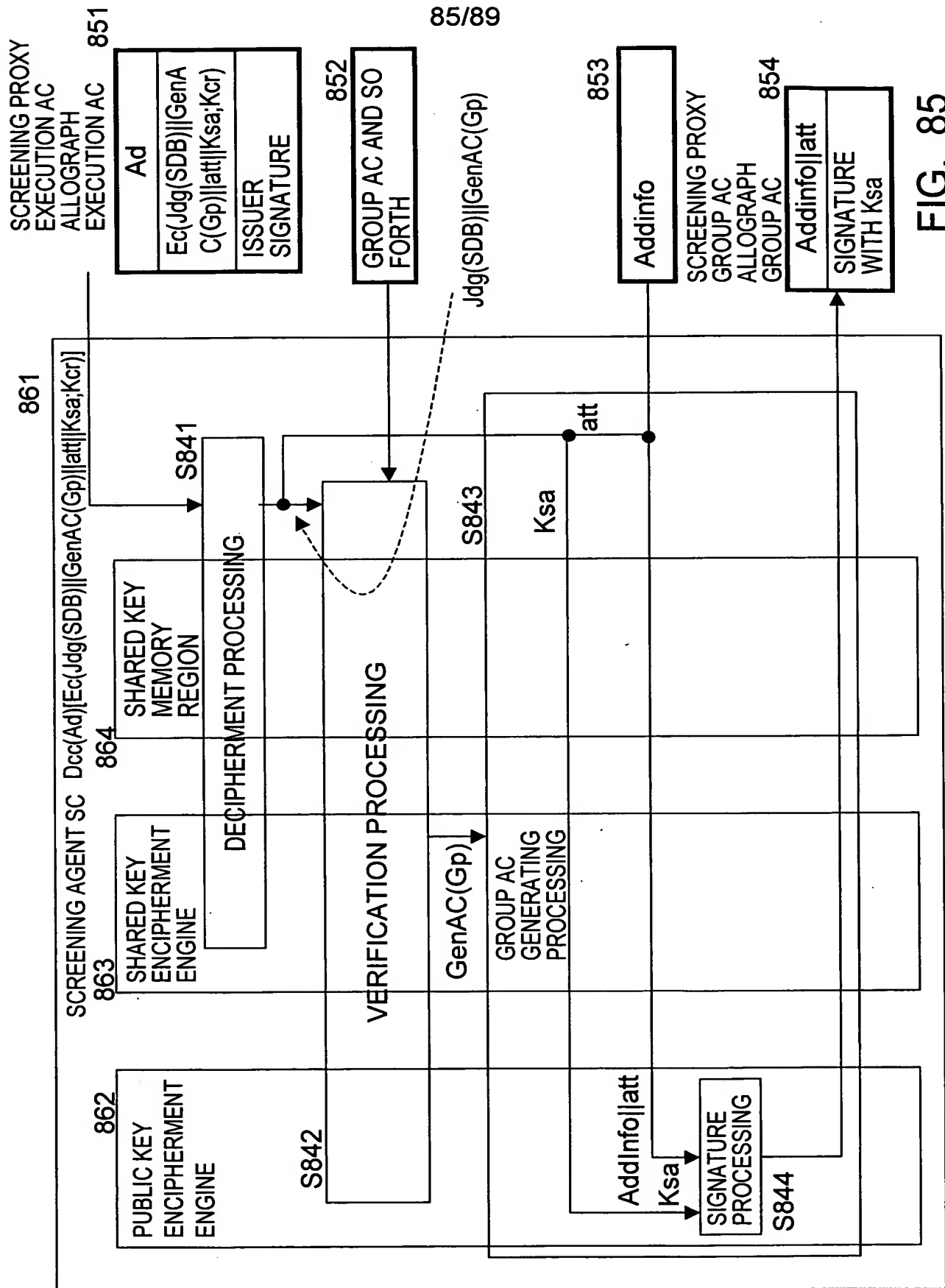


FIG. 85

FIG. 86

87/89

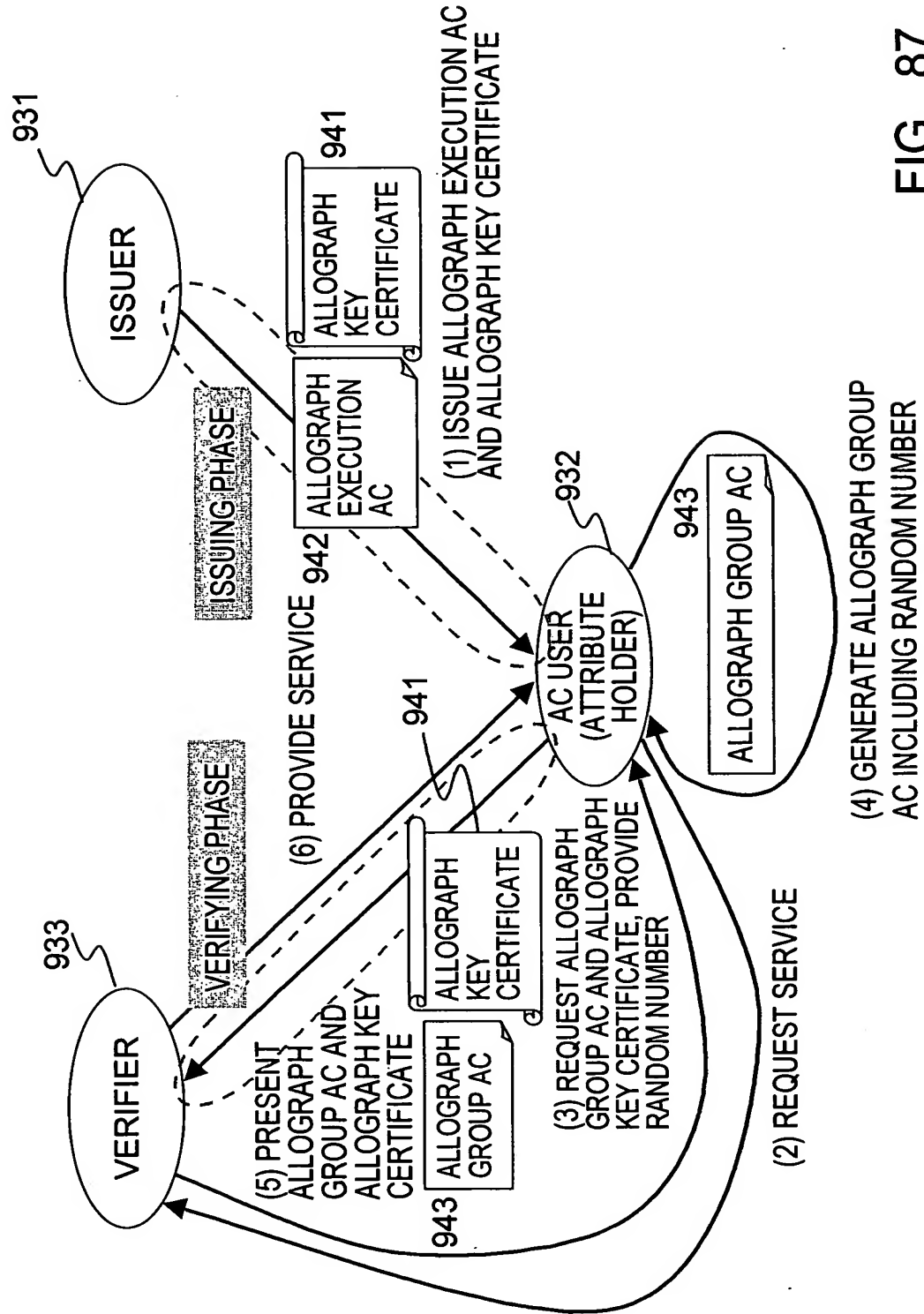


FIG. 87

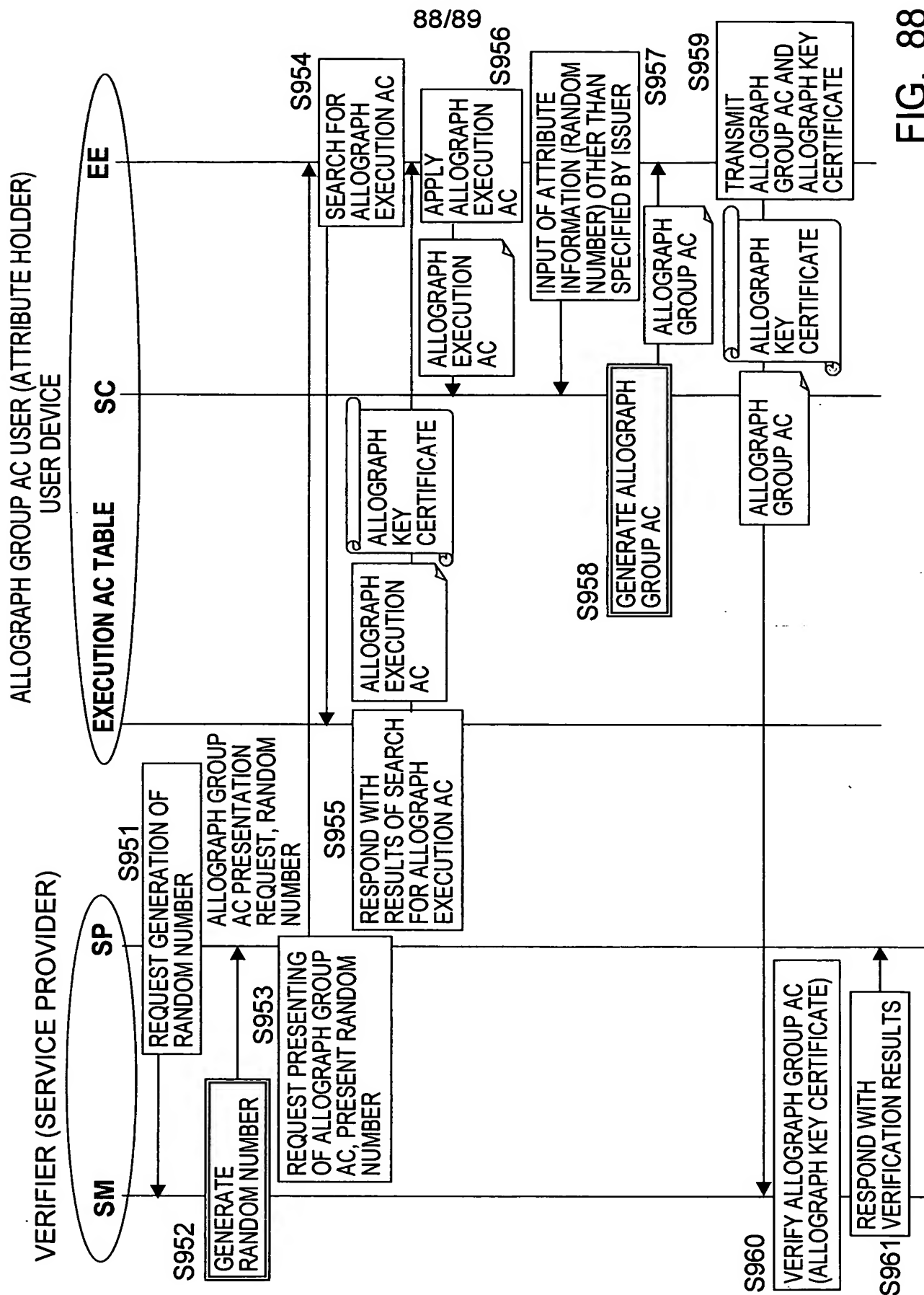


FIG. 88

89/89

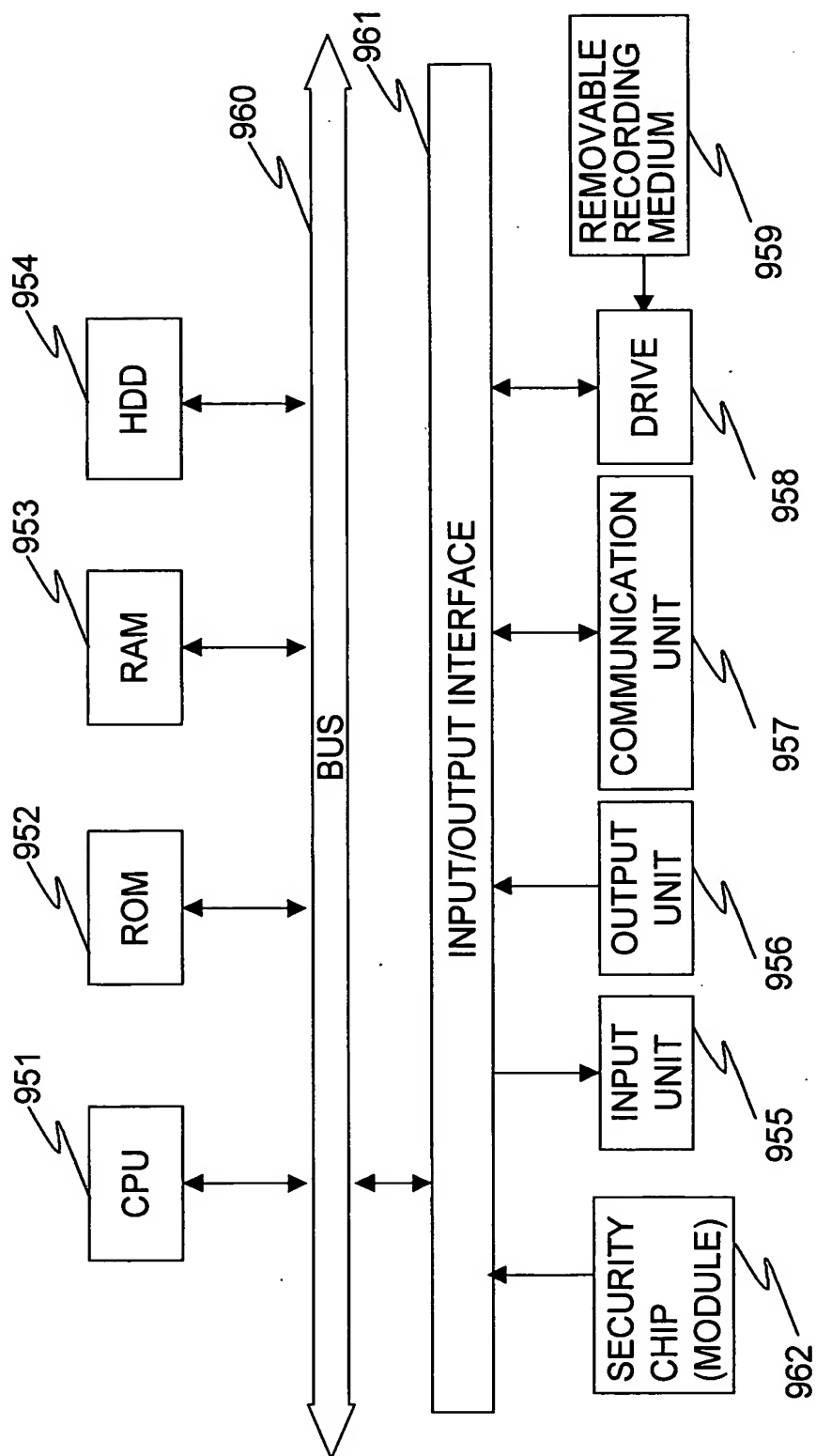


FIG. 89